

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Keiichi TAKAGAKI et al. :
Serial No. NEW : **Attn: APPLICATION BRANCH**
Filed October 30, 2003 : Attorney Docket No. 2003_1574A

COMMUNICATION DEVICE,
COMMUNICATION SYSTEM, AND
ALGORITHM SELECTION METHOD

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450


Sir:

Applicants in the above-entitled application hereby claim the dates of priority under the International Convention of Japanese Patent Application No. 2002-318189, filed October 31, 2002, and Japanese Patent Application No. 2003-023797, filed January 31, 2003, as acknowledged in the Declaration of this application.

Certified copies of said Japanese Patent Applications are submitted herewith.

Respectfully submitted,

Keiichi TAKAGAKI et al.

By 
Charles R. Watts
Registration No. 33,142
Attorney for Applicants

CRW/asd
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
October 30, 2003

(

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 3 1 日
Date of Application:

出 願 番 号 特 願 2 0 0 2 - 3 1 8 1 8 9
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 3 1 8 1 8 9]

出 願 人 松 下 電 器 産 業 株 式 会 社
Applicant(s):

2 0 0 3 年 9 月 1 6 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 7 5 8 4 7

【書類名】 特許願

【整理番号】 2032740085

【提出日】 平成14年10月31日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/22

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 高垣 景一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 横田 博史

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 五島 雪絵

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 辻 敦宏

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 アルゴリズム選択方法および通信システムおよび通信装置

【特許請求の範囲】

【請求項 1】 CPUを用いて暗号アルゴリズムの処理を行うシステムにおいて、

複数の暗号アルゴリズムの各々について、暗号処理を行ったときに、システム全体で必要となるCPUリソースを全処理負荷として推定する全処理負荷推定手順と、

各々の暗号アルゴリズムについて、前記全処理負荷と、第一基準値とを比較する比較手順と、

前記全処理負荷が前記第一基準値を下回る、ひとつもしくは複数の暗号アルゴリズムを選択する選択手順とを有することを特徴とするアルゴリズム選択方法。

【請求項 2】 前記全処理負荷のうち、

暗号処理を必要とするアプリケーションの実行に必要と推定されるCPUリソースを暗号アプリケーション負荷とし、

同一CPU上で実行されるその他の全ての処理に必要と推定されるCPUリソースを非暗号アプリケーション負荷とし、

各々の暗号アルゴリズムに対する前記全処理負荷推定手順は、

前記暗号アプリケーション負荷を推定する暗号アプリケーション負荷推定手順と、

前記非暗号アプリケーション負荷を推定する、非暗号アプリケーション負荷推定手順と、

各々の暗号アルゴリズムについて、前記暗号アプリケーション負荷と前記非暗号アプリケーション負荷との合計を求める手順とにより構成されることを特徴とする請求項 1 に記載のアルゴリズム選択方法。

【請求項 3】 前記選択手順は、

前記全処理負荷が前記第一基準値を下回る複数の暗号アルゴリズムを選択する低処理負荷暗号アルゴリズム選択手順と、

前記手順によって選択された複数の暗号アルゴリズムの暗号強度の順序を求め

る手順と、

前記低処理負荷暗号アルゴリズムのなかで、暗号強度の高いものからひとつまたは複数の暗号アルゴリズムを選択する手順とにより構成されることを特徴とする請求項 1 または 2 に記載のアルゴリズム選択方法。

【請求項 4】暗号アルゴリズムを選択するときに、暗号処理を必要とするアプリケーションが実行されていない場合において、

前記非暗号アプリケーション負荷推定手順は、

その時点までの一定期間における測定された CPU 使用率の平均値を前記非暗号アプリケーション負荷として用いる手順であることを特徴とする請求項 2 に記載のアルゴリズム選択方法。

【請求項 5】暗号アルゴリズムを選択するときに、暗号処理を必要とするアプリケーションが実行中である場合において、

前記非暗号アプリケーション負荷推定手順は、

その時点までの一定期間における測定された CPU 使用率の平均値を求める手順と、

その時点で使用している暗号アルゴリズムを用いて前記暗号処理を必要とするアプリケーションを実行するのに必要と推定される CPU リソースを現暗号アプリケーション負荷として求める手順と、

前記 CPU 使用率から前記現暗号アプリケーション負荷を引いた値を前記非暗号アプリケーション負荷として用いる手順とにより構成されることを特徴とする請求項 2 に記載のアルゴリズム選択方法。

【請求項 6】前記非暗号アプリケーション負荷推定手順は、その時点で実行されている複数の非暗号アプリケーションが、過去に同じ組み合わせで実行されていた期間の CPU 使用率の平均値を求め、その値を前記非暗号アプリケーション負荷として用いる手順であることを特徴とする請求項 2 に記載のアルゴリズム選択方法。

【請求項 7】前記非暗号アプリケーション負荷推定手順は、あらかじめシステムによって既定される値を求め、その値を前記非暗号アプリケーション負荷として用いる手順であることを特徴とする請求項 2 に記載のアルゴリズム選択方法。

【請求項 8】前記暗号アプリケーション負荷推定手順は、過去に、各々の暗号アルゴリズムを用いて、前記暗号処理を必要とするアプリケーションのみを実行していた期間の、CPU 使用率の平均値を求め、その値を前記暗号アプリケーション負荷として用いる手順であることを特徴とする請求項 2 に記載のアルゴリズム選択方法。

【請求項 9】前記暗号アプリケーション負荷推定手順は、各々の暗号アルゴリズムごとに、あらかじめシステムによって既定される値を、前記暗号アプリケーション負荷として用いる手順であることを特徴とする請求項 2 に記載のアルゴリズム選択方法。

【請求項 10】CPU を用いて暗号処理を行うシステムにおいて、暗号処理実行中の任意の時刻に、その時点までの一定期間に測定した CPU 使用率の平均値を求める手順と、

前記 CPU 使用率と第二基準値とを比較する手順と、

比較の結果前記 CPU 使用率が第二基準値よりも高い場合は、その時点で使用している暗号アルゴリズムよりも、負荷の低い一つもしくは複数の暗号アルゴリズムを選択する手順とを有することを特徴とするアルゴリズム選択方法。

【請求項 11】利用可能な複数の暗号アルゴリズムの暗号強度の順序を求める手順と、

前記 CPU 使用率と第三基準値とを比較し、前記 CPU 使用率が第三基準値よりも低い場合は、その時点で使用している暗号アルゴリズムよりも、暗号強度の高い一つもしくは複数の暗号アルゴリズムを選択する手順と、

をさらに有することを特徴とする請求項 10 に記載のアルゴリズム選択方法。

【請求項 12】前記 CPU 使用率と第二基準値および第三基準値とを比較し、前記 CPU 使用率が第二基準値より低く第三基準値より高い場合は、その時点で使用している暗号アルゴリズムを選択する手順をさらに有することを特徴とする請求項 10 または 11 に記載のアルゴリズム選択方法。

【請求項 13】前記暗号処理を行なう暗号アルゴリズムの代りとして、認証処理を行なう認証アルゴリズム、圧縮伸長処理を行なう圧縮アルゴリズム、の少なくとも一方を適用したことを特徴とする、請求項 1～12 のいずれかに記載のア

ルゴリズム選択方法。

【請求項 14】前記各種負荷推定手順もしくはCPU使用率取得手順のうち少なくとも一つは、予め用意されたCPU使用率情報を適用することを特徴とする、請求項 1～12のいずれかに記載のアルゴリズム選択方法。

【請求項 15】通信データに暗号処理を施して通信を行なう暗号通信において、第1の通信装置と、別の第2の通信装置との間で暗号通信を行い、前記暗号通信に用いる暗号アルゴリズムを、一方の通信装置からの提案とその提案に対する他方の通信装置からの応答という形で折衝するシステムであって、

前記第1の通信装置は、

前記第1の通信装置が利用可能な複数の暗号アルゴリズムから、請求項 1～14のいずれかに記載のアルゴリズム選択方法を利用して、一つもしくは複数の暗号アルゴリズムを選択する手段と、

選択した前記暗号アルゴリズムを通信相手に提案する手段と、

通信相手から応答された暗号アルゴリズムを用いて暗号処理を、CPUを用いて行う手段とを含み、

前記第2の通信装置は、

通信相手から提案された一つまたは複数の暗号アルゴリズムから一つを選ぶ選択手段と、

前記選択手段により選択した暗号アルゴリズムを通信相手に応答する応答手段と、

前記選択手段により選択した暗号アルゴリズムを用いて暗号処理を行う手段とを含むことを特徴とする通信システム。

【請求項 16】通信データに暗号処理を施して通信を行なう暗号通信において、第1の通信装置と、別の第2の通信装置との間で、暗号通信を行い、前記暗号通信に用いる暗号アルゴリズムを、一方からの提案とその提案に対する応答という形で折衝するシステムであって、

前記第1の通信装置は、

前記第2の通信装置が提案してきた複数の暗号アルゴリズムから、請求項 1～14のいずれかに記載のアルゴリズム選択方法を利用して、一つの暗号アルゴリ

ズムを選択する手段と、

選択した前記暗号アルゴリズムを通信相手に応答する手段と、

応答した暗号アルゴリズムを用いた暗号処理を、CPUを用いて行う手段とを含み、

前記第2の通信装置は、

一つまたは複数の暗号アルゴリズムを提案する手段と、

通信相手から応答された暗号アルゴリズムを用いて暗号処理を行う手段とを含むことを特徴とする通信システム。

【請求項17】通信データに暗号処理を施して通信を行なう暗号通信において、第1の通信装置と、別の第2の通信装置との間で、暗号通信を行い、前記暗号通信に用いる暗号アルゴリズムを、一方からの提案とその提案に対する応答という形で折衝するシステムであって、

前記第1の通信装置は、

暗号通信途中に、現在時点で使用している暗号アルゴリズムを過去に通信相手と折衝したときに、その折衝時点直後からの一定期間に測定したCPU使用率の平均値を記憶しておく折衝直後CPU使用率記憶手段と、

前記現在時点までの一定期間に測定したCPU使用率の平均値を求める手段と、

前記折衝直後CPU使用率記憶手段により記憶されたCPU使用率と現在時点でのCPUとが変化していることを検出する手段と、

前記CPU使用率の変化を検出したときに、請求項1～14のいずれかに記載のアルゴリズム選択方法を利用して、一つもしくは複数の暗号アルゴリズムを選択する手段と、

選択した前記暗号アルゴリズムが、既に使用している暗号アルゴリズムと異なれば、前記暗号アルゴリズムを通信相手に提案する手段と、

通信相手から応答された暗号アルゴリズムを用いて暗号処理を、CPUを用いて行う手段とを含み、

前記第2の通信装置は、

通信相手から提案された一つまたは複数の暗号アルゴリズムから一つを選ぶ選

択手段と、

前記選択手段により選択した暗号アルゴリズムを通信相手に応答通知する応答手段と、

前記選択手段により選択した暗号アルゴリズムを用いて暗号処理を行う手段とを含むことを特徴とする通信システム。

【請求項 18】 通信データに暗号処理を施して通信を行なう暗号通信において、第 1 の通信装置と、別の第 2 の通信装置との間で暗号通信を行い、前記暗号通信において同時に複数の暗号アルゴリズムを使用可能であるシステムであって、

前記第 1 の通信装置は、

暗号通信時の暗号処理を、CPU を用いて行う手段と、

暗号処理が必要な通信データ送信時に、使用可能な複数の暗号アルゴリズムから、請求項 1 ～ 14 のいずれかに記載のアルゴリズム選択方法を利用して、一つの暗号アルゴリズムを選択する手段と、

選択した前記暗号アルゴリズムを用いて前記送信データに暗号処理を施す手段とを含み、

前記第 2 の通信装置は、

受信したデータに用いられている暗号アルゴリズムを用いて、暗号処理を行う手段を含むことを特徴とする通信システム。

【請求項 19】 通信データに暗号処理を施して通信を行なう暗号通信において、第 1 の通信装置と、別の第 2 の通信装置との間で暗号通信を行い、また一つの暗号通信において同時に複数の暗号アルゴリズムを使用可能であるシステムであって、

前記第 1 の通信装置は、

暗号通信時の暗号処理を、CPU を用いて行う手段と、

使用可能な複数の暗号アルゴリズムから、請求項 1 ～ 14 のいずれかに記載のアルゴリズム選択方法を利用して、一つの暗号アルゴリズムを選択する手段と、

選択した前記暗号アルゴリズムを、前記第 2 の通信装置に通知する手段と、

受信したデータに用いられている暗号アルゴリズムを用いて、暗号処理を行う手段とを含み、

前記第 2 の通信装置は、

通知された前記暗号アルゴリズムを用いて前記送信データに暗号処理を施す手段を含むことを特徴とする通信システム。

【請求項 20】 上記暗号処理を行なう暗号アルゴリズムの代りとして、認証処理を行なう認証アルゴリズム、圧縮伸長処理を行なう圧縮アルゴリズム、の少なくとも一方を適用したことを特徴とする、請求項 15～19 のいずれかに記載の通信システム。

【請求項 21】 通信データに暗号処理を施して通信を行なう暗号通信において、第 1 の通信装置は、別の第 2 の通信装置との間で暗号通信を行い、前記暗号通信に用いる暗号アルゴリズムを、一方の通信装置からの提案とその提案に対する他方の通信装置からの応答という形で折衝する通信装置であって、

前記第 1 の通信装置は、

前記第 1 の通信装置が利用可能な複数の暗号アルゴリズムから、請求項 1～14 のいずれかに記載のアルゴリズム選択方法を利用して、一つもしくは複数の暗号アルゴリズムを選択する手段と、

選択した前記暗号アルゴリズムを通信相手に提案する手段と、

通信相手から応答された暗号アルゴリズムを用いて暗号処理を、CPU を用いて行う手段とを含むことを特徴とする通信装置。

【請求項 22】 通信データに暗号処理を施して通信を行なう暗号通信において、第 1 の通信装置は、別の第 2 の通信装置との間で、暗号通信を行い、前記暗号通信に用いる暗号アルゴリズムを、一方からの提案とその提案に対する応答という形で折衝する通信装置であって、

前記第 1 の通信装置は、

前記第 2 の通信装置が提案してきた複数の暗号アルゴリズムから、請求項 1～14 のいずれかに記載のアルゴリズム選択方法を利用して、一つの暗号アルゴリズムを選択する手段と、

選択した前記暗号アルゴリズムを通信相手に応答する手段と、

応答した暗号アルゴリズムを用いた暗号処理を、CPU を用いて行う手段とを含むことを特徴とする通信装置。

【請求項 23】通信データに暗号処理を施して通信を行なう暗号通信において、第1の通信装置は、別の第2の通信装置との間で、暗号通信を行い、前記暗号通信に用いる暗号アルゴリズムを、一方からの提案とその提案に対する応答という形で折衝する通信装置であって、

前記第1の通信装置は、

暗号通信途中に、現在時点で使用している暗号アルゴリズムを過去に通信相手と折衝したときに、その折衝時点直後からの一定期間に測定したCPU使用率の平均値を記憶しておく折衝直後CPU使用率記憶手段と、

前記現在時点までの一定期間に測定したCPU使用率の平均値を求める手段と、

前記折衝直後CPU使用率記憶手段により記憶されたCPU使用率と現在時点でのCPUとが変化していることを検出する手段と、

前記CPU使用率の変化を検出したときに、請求項1～14のいずれかに記載のアルゴリズム選択方法を利用して、一つもしくは複数の暗号アルゴリズムを選択する手段と、

選択した前記暗号アルゴリズムが、既に使用している暗号アルゴリズムと異なれば、前記暗号アルゴリズムを通信相手に提案する手段と、

通信相手から応答された暗号アルゴリズムを用いて暗号処理を、CPUを用いて行う手段とを含むことを特徴とする通信装置。

【請求項 24】通信データに暗号処理を施して通信を行なう暗号通信において、第1の通信装置は、別の第2の通信装置との間で暗号通信を行い、前記暗号通信において同時に複数の暗号アルゴリズムを使用可能である通信装置であって、前記第1の暗号通信装置は、

暗号通信時の暗号処理を、CPUを用いて行う手段と、

暗号処理が必要な通信データ送信時に、使用可能な複数の暗号アルゴリズムから、請求項1～14のいずれかに記載のアルゴリズム選択方法を利用して、一つの暗号アルゴリズムを選択する手段と、

選択した前記暗号アルゴリズムを用いて前記送信データに暗号処理を施す手段とを含むことを特徴とする通信装置。

【請求項 25】 通信データに暗号処理を施して通信を行なう暗号通信において、第 1 の通信装置は、別の第 2 の通信装置との間で暗号通信を行い、また一つの暗号通信において同時に複数の暗号アルゴリズムを使用可能である通信装置であって、

前記第 1 の通信装置は、

暗号通信時の暗号処理を、CPU を用いて行う手段と、

使用可能な複数の暗号アルゴリズムから、請求項 1 ～ 14 のいずれかに記載のアルゴリズム選択方法を利用して、一つの暗号アルゴリズムを選択する手段と、

選択した前記暗号アルゴリズムを、前記第 2 の通信装置に通知する手段と、

受信したデータに用いられている暗号アルゴリズムを用いて、暗号処理を行う手段とを含むことを特徴とする通信装置。

【請求項 26】 上記暗号処理を行なう暗号アルゴリズムの代りとして、認証処理を行なう認証アルゴリズム、圧縮伸長処理を行なう圧縮アルゴリズム、の少なくとも一方を適用したことを特徴とする、請求項 21 ～ 25 のいずれかに記載の通信装置。

【請求項 27】 請求項 1 ～ 14 のいずれかに記載のアルゴリズム選択方法を、コンピュータに機能させるためのプログラムとして記録した記録媒体。

【請求項 28】 請求項 1 ～ 14 のいずれかに記載のアルゴリズム選択方法を、コンピュータに機能させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、暗号通信などのデータの通信を行う際に使用する暗号・認証・圧縮などのアルゴリズムを選択する方法に関する。

【0002】

【従来の技術】

<ネット家電>

近年のインターネット技術の普及に伴い、携帯端末や家電製品などをインターネットに接続し、さまざまなサービスを展開しようという動きが活発になってい

る。インターネットに接続可能な家電製品のさきがけとして、現在 e p ステーションのような通信機能付き録画機能付き家電機器が発売されている。その e p ステーションは、図 1 8 で示されるような e p サービスを実現するための機器である。e p サービスの特徴は次の 2 つである。まず、放送局と e p ステーションをインターネットで結ぶことにより、放送と通信を融合したサービス、例えば T V ショッピングや視聴者参加型番組などを実現することができる。また、e p ステーションはハードディスクを備えるため、衛星から放送された T V 番組や広告データ、インターネットから受信した電子メールデータなどを蓄積することができる。

【 0 0 0 3 】

現在の e p ステーションでは、電話回線を用いてインターネットに接続している。しかし、A D S L や C A T V、光ファイバーなどの高速回線の普及によって、家庭においても高速なインターネット接続環境が整いつつあり、今後高速通信が可能な e p ステーションの後継機が登場することは容易に想像できる。

【 0 0 0 4 】

非特許文献 1 では、e p サービスの前身である e プロットフォーム構想について述べられており、高画質放送とデータ放送、蓄積放送サービスやインターネットへの高速アクセスを連動させたサービスの形態が示されている。高速インターネットを利用したアプリケーションとしては、映像配信や音楽配信などのダウンロードサービス、テレビ電話やネットワークカメラによる監視などが考えられる。

【 0 0 0 5 】

この中でネットワークカメラを利用する場合を考える。ネットワークカメラの民生用の利用法としては、保育所にいる子供の様子や、独居老人となっている親の様子、外出中の自宅の様子などを観察するなどが考えられる。このようなプライバシーを伴うような映像をインターネット上で盗み見られないようにするためには、映像データを暗号化などにより保護する必要がある。

【 0 0 0 6 】

< 暗号通信 >

従来から、機密性が必要とされるデータをインターネットなどの公衆ネットワーク上でやりとりする場合には、データの暗号化処理が行われている。非特許文献2では、インターネット上に潜む危険と、その対策としての、暗号や認証の技術について詳しく述べられている。また、非特許文献3等には、インターネットで用いられている代表的な暗号化・認証プロトコルである、IPsec (Internet Protocol Security) について詳細に述べられている。以下では、暗号通信の一般的な処理の流れを説明する。まず、双方において同じ暗号アルゴリズムを設定する。また、双方において、暗号化鍵と通信相手が暗号化したデータを復号化するための復号化鍵を設定する。なお、暗号アルゴリズムや鍵の設定は手動での設定、もしくは双方での間の自動ネゴシエーションによって行われる。以上の設定が完了すると、次のような手順で暗号通信が行われる。まず、データ送信側は、送信データを設定された暗号アルゴリズムと暗号化鍵を用いて暗号化し、インターネットに送信する。受信側は、暗号化されたパケットを受信すると、設定された暗号アルゴリズムと復号化鍵を用いて、暗号化パケットを復号化する。

【0007】

データ送信側とデータ受信側が同じ暗号アルゴリズムを使用するためには、双方の間で、上記のネゴシエーションが行われる。図20は、従来の方法でネゴシエーションを行なう要部のブロック図である。通信機能部215は、相手の通信機能部との間で、各種データをパケット形式にして通信を行なう。暗号アルゴリズムのネゴシエーションにおいては、ネゴシエーション用のパケットを、相手との間でやり取りする。暗号アルゴリズムネゴシエーション機能部220内の、ネゴシエーションパケット作成・解釈部217は、送信時には、暗号アルゴリズム選択部219の指示に基づき、送信用のネゴシエーションパケットを所定の形式で作成し、受信時には、受信したネゴシエーションパケットの内容を解釈して暗号アルゴリズム選択部219に入手情報を渡す。また、暗号アルゴリズム選択部219は、決定した暗号アルゴリズムを暗号アルゴリズム設定部218に知らせ、アルゴリズム設定を指示する。暗号処理機能部216は、設定された暗号アルゴリズムを使用してデータの暗号化や復号化を行なう。このような従来のネゴ

シエーションでは、暗号アルゴリズム選択部 219 は、暗号アルゴリズムの提案を行なう場合には、保有している暗号アルゴリズムから、ユーザによって設定された、又はプログラム中であらかじめ定められている、ひとつ又は複数の暗号アルゴリズムを選んで相手に提案する。また、相手から提案を受けた場合は、その提案に対する応答として、保有している暗号アルゴリズムの中で最も高優先度の暗号アルゴリズムを選択し、通知するようにしている。

【0008】

【非特許文献 1】

野村敦子著、「ブロードバンド革命―目指せ！ユビキタス・ネットワーク社会」、初版、中央経済社、平成13年4月1日、p. 225-227 (ISBN 4-502-57211-X)

【非特許文献 2】

ユーリス・ブラック著、波多浩昭、松本直人訳、「インターネットセキュリティガイド」、初版、ピアソン・エデュケーション発行、2001年11月20日、全頁 (ISBN 4-89471-455-8)

【非特許文献 3】

「RFC 2401」、IETF (Internet Engineering Task Force) 発行

【0009】

【発明が解決しようとする課題】

ここで、前述した通信機能付き録画機能付き家電機器で、暗号通信を必要とするネットワークカメラのような機能を使いながら、受像機能部により受信したTV放送データを録画する場合を考える。暗号通信で行われる暗号処理は、対象データに対して複雑な処理を行う必要がある。このため、暗号通信は、暗号化を行わない通信に比べて、非常に処理負荷が高くなることが知られている。ネットワークカメラデータの復号化処理と録画という、リアルタイムに処理しなければならない高負荷な処理が重なった場合、前述の図20のようなネゴシエーションでは、内蔵CPUの処理能力では、両方を同時には処理しきれない可能性がある。つまり、TV放送の録画に失敗するか、もしくは、ネットワークカメラの画像が

乱れたり止まったりするという問題が発生することがある。図2は、このときの内蔵CPUの処理能力と、ネットワークカメラおよびTV録画に必要なCPUリソースの関係を表している。つまり、図2のようにネットワークカメラに必要なCPUリソースと、TV録画に必要なCPUリソースの合計が、内蔵CPUの処理能力を越えた場合に、上記のような問題が発生する。

【0010】

本発明の目的は、暗号通信処理と他の高負荷な処理を同時に行わなければならない場合に、できるだけ強固な機密性を提供しつつも、暗号処理の負荷を軽減し、CPUリソースの枯渇によって生じる上記のような問題を解決する方法を提供することである。

【0011】

【課題を解決するための手段および発明の効果】

請求項1の発明は、暗号アルゴリズムを選択する方法であって、CPUを用いて暗号処理を行うシステムにおいて、複数の暗号アルゴリズムの各々について、暗号処理を行ったときに、システム全体で必要となるCPUリソースを全処理負荷として推定する全処理負荷推定手順と、各々の暗号アルゴリズムについて、前記全処理負荷と第一基準値とを比較する比較手順と、前記全処理負荷が、前記第一基準値を下回る、ひとつもしくは複数の暗号アルゴリズムを選択する選択手順とを有することを特徴とする。

【0012】

上記請求項1の発明により選択された暗号アルゴリズムを用いて、暗号処理を行えば、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。

【0013】

請求項2の発明は、請求項1の暗号アルゴリズムを選択する方法であって、前記全処理負荷を、暗号処理を必要とするアプリケーションの実行に必要と推定されるCPUリソースと、同一CPU上で実行されるその他の全ての処理に必要と推定されるCPUリソースの合計とし、各々の暗号アルゴリズムに対する前記全処理負荷推定手順は、暗号処理を必要とするアプリケーションの実行に必要とさ

れるCPUリソースを暗号アプリケーション負荷として推定する暗号アプリケーション負荷推定手順と、前記暗号処理で利用されるのと同じCPUを利用する、暗号処理を必要としない他の全ての処理に必要とされるCPUリソースを非暗号アプリケーション負荷として推定する非暗号アプリケーション負荷推定手順と、各々の暗号アルゴリズムについて、前記暗号アプリケーション負荷と前記非暗号アプリケーション負荷との合計を求める手順、とにより構成されることを特徴とする。

【0014】

上記請求項2の発明により選択された暗号アルゴリズムを用いて、暗号処理を行えば、簡単な計算により、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。

【0015】

請求項3の発明は、請求項1または請求項2の暗号アルゴリズムを選択する方法であって、前記選択手順は、前記全処理負荷が前記第一基準値を下回る複数の暗号アルゴリズムを選択する低処理負荷暗号アルゴリズム選択手順と、前記手順によって選択された複数の暗号アルゴリズムの暗号強度の順序を求める手順と、前記低処理負荷暗号アルゴリズムのなかで、暗号強度の高いものからひとつまたは複数の暗号アルゴリズムを選択する手順とにより構成されることを特徴とする。

【0016】

上記請求項3の発明により選択された暗号アルゴリズムを用いて、暗号処理を行えば、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぎつつ、できるだけ強固な暗号アルゴリズムを使用して暗号処理を行うことができる。

【0017】

請求項4の発明は、請求項2の暗号アルゴリズムを選択する方法であって、暗号アルゴリズムを選択するときに、暗号処理を必要とするアプリケーションが実行されていない場合において、前記非暗号アプリケーション負荷推定手順は、その時点までの一定期間における測定されたCPU使用率の平均値を、その値を前

記非暗号アプリケーション負荷として用いる手順であることを特徴とする。

【0018】

上記請求項4の発明により選択された暗号アルゴリズムを用いて、暗号処理を行えば、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。さらに、前記暗号アルゴリズムを選択する際には、前記非暗号アプリケーション負荷があらかじめシステムによって既定されていなくてもよい。

【0019】

請求項5の発明は、請求項2の暗号アルゴリズムを選択する方法であって、暗号アルゴリズムを選択するときに、暗号処理を必要とするアプリケーションが実行中である場合において、前記非暗号アプリケーション負荷推定手順は、その時点までの一定期間における測定されたCPU使用率の平均値を求める手順と、その時点で使用している暗号アルゴリズムを用いて前記暗号処理を必要とするアプリケーションを実行するのに必要と推定されるCPUリソースを現暗号アプリケーション負荷として求める手順と、前記CPU使用率から前記現暗号アプリケーション負荷を引いた値を前記非暗号アプリケーション負荷として用いる手順とにより構成されることを特徴とする。

【0020】

上記請求項5の発明により選択された暗号アルゴリズムを用いて、暗号処理を行えば、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。さらに、前記暗号アルゴリズムを選択する際には、前記非暗号アプリケーション負荷があらかじめシステムによって既定されていなくてもよい。

【0021】

請求項6の発明は、請求項2の暗号アルゴリズムを選択する方法であって、前記非暗号アプリケーション負荷推定手順は、その時点で実行されている複数の非暗号アプリケーションが、過去に同じ組み合わせで実行されていた期間の、CPU使用率の平均値を求め、その値を前記非暗号アプリケーション負荷として用いる手順であることを特徴とする。

【0022】

上記請求項6の発明により選択された暗号アルゴリズムを用いて、暗号処理を行えば、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。さらに、前記暗号アルゴリズムを選択する際には、前記非暗号アプリケーション負荷があらかじめシステムによって既定されていなくてもよい。

【0023】

請求項7の発明は、請求項2の暗号アルゴリズムを選択する方法であって、前記非暗号アプリケーション負荷推定手順は、あらかじめシステムによって既定される値を求め、その値を前記非暗号アプリケーション負荷として用いる手順であることを特徴とする。

【0024】

上記請求項7の発明により選択された暗号アルゴリズムを用いて、暗号処理を行えば、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。さらに、前記暗号アルゴリズムを選択する際に、非暗号アプリケーション負荷を求めるためにCPU使用率を測定する必要がない。

【0025】

請求項8の発明は、請求項2の暗号アルゴリズムを選択する方法であって、前記暗号アプリケーション負荷推定手順は、過去に、各々の暗号アルゴリズムを用いて、前記暗号処理を必要とするアプリケーションのみを実行していた期間の、CPU使用率の平均値を求め、その値を前記暗号アプリケーション負荷として用いる手順であることを特徴とする。

【0026】

上記請求項8の発明により選択された暗号アルゴリズムを用いて、暗号処理を行えば、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。さらに、前記暗号アルゴリズムを選択する際には、前記暗号アプリケーション負荷があらかじめシステムによって既定されていなくてもよい。

【0027】

請求項9の発明は、請求項2の暗号アルゴリズムを選択する方法であって、前記暗号アプリケーション負荷推定手順は、各々の暗号アルゴリズムごとに、あらかじめシステムによって既定される値を求め、その値を前記暗号アプリケーション負荷として用いる手順であることを特徴とする。

【0028】

上記請求項9の発明により選択された暗号アルゴリズムを用いて、暗号処理を行えば、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。さらに、前記暗号アルゴリズムを選択する際に、暗号アプリケーション負荷を求めるためにCPU使用率を測定する必要がない。

【0029】

請求項10の発明は、暗号アルゴリズムを選択する方法であって、CPUを用いて暗号処理を行うシステムにおいて、暗号処理実行中の任意の時刻に、その時点までの一定期間に測定したCPU使用率の平均値を求める手順と、前記CPU使用率と第二基準値とを比較する手順と、利用可能な複数の暗号アルゴリズムの暗号強度の順序を求める手順と、比較の結果前記CPU使用率が第二基準値よりも高い場合は、その時点で使用している暗号アルゴリズムよりも、負荷の低い一つもしくは複数の暗号アルゴリズムを選択する手順とを有することを特徴とする。

【0030】

上記請求項10の発明による暗号アルゴリズムの選択を繰り返すことにより、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。

【0031】

請求項11の発明は、請求項10の暗号アルゴリズムを選択する方法であって、前記CPU使用率と第三基準値とを比較し、前記CPU使用率が第三基準値よりも低い場合は、その時点で使用している暗号アルゴリズムよりも、暗号強度の高い一つもしくは複数の暗号アルゴリズムを選択する手順を、さらに有すること

を特徴とする。

【0032】

上記請求項11の発明による暗号アルゴリズムの選択を繰り返すことにより、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぎつつ、できるだけ強固な暗号アルゴリズムを使用して暗号処理を行うことができる。

【0033】

請求項12の発明は、請求項10または請求項11の暗号アルゴリズムを選択する方法であって、前記CPU使用率と第二基準値および第三基準値とを比較し、前記CPU使用率が第二基準値より低く第三基準値より高い場合は、その時点で使用している暗号アルゴリズムを選択する手順を、さらに有することを特徴とする。

【0034】

上記請求項12の発明による暗号アルゴリズムの選択を繰り返すことにより、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぎつつ、できるだけ強固な暗号アルゴリズムを使用して暗号処理を行うことができる。

【0035】

請求項13によれば、本発明は、暗号アルゴリズム以外のアルゴリズムにおける選択にも適用可能である。

【0036】

請求項14によれば、CPU使用率の推定は、可能な時点で行なえる。

【0037】

請求項15の発明は、通信システムであって、暗号通信時の暗号処理を、CPUを用いて行う第1の通信装置と、別の第2の通信装置との間で暗号通信を行い、前記暗号通信に用いる暗号アルゴリズムを、一方からの提案とその提案に対する応答という形で折衝するシステムであって、前記第1の通信装置は、前記第1の通信装置が利用可能な複数の暗号アルゴリズムから、請求項1～14のいずれかに記載のアルゴリズム選択方法を利用して、一つもしくは複数の暗号アルゴリ

ズムを選択する手段と、選択した前記暗号アルゴリズムを通信相手に提案する手段とを含むことを特徴とする。

【0038】

上記請求項15の発明によれば、前記第1の通信装置は、暗号通信に用いる暗号アルゴリズムを折衝する際に、前記第2の通信装置から提案された暗号アルゴリズムの中から、CPUリソースの不足によって前記第1の通信装置で動作するアプリケーションの実行に支障が出ることを防ぐことができるような暗号アルゴリズムを選択し、前記第2の通信装置に対して応答することができる。

【0039】

請求項16の発明は、暗号通信システムであって、暗号通信時の暗号処理を、CPUを用いて行う第1の通信装置と、別の第2の通信装置との間で、暗号通信を行い、前記暗号通信に用いる暗号アルゴリズムを、一方からの提案とその提案に対する応答という形で折衝するシステムであって、前記第2の通信装置は、複数の暗号アルゴリズムを提案する手段を含み、前記第1の通信装置は、前記第2の通信装置が提案してきた複数の暗号アルゴリズムから、請求項1～14のいずれかに記載のアルゴリズム選択方法を利用して、一つもしくは複数の暗号アルゴリズムを選択する手段と、選択した前記暗号アルゴリズムを通信相手に応答通知する手段とを含むことを特徴とする。

【0040】

上記請求項16の発明によれば、前記第1の通信装置は、暗号通信に用いる暗号アルゴリズムを折衝する際に、CPUリソースの不足によって前記第1の通信装置で動作するアプリケーションの実行に支障が出ることを防ぐことができるような暗号アルゴリズムを、前記第2の通信装置に対して提案することができる。

【0041】

請求項17の発明は、暗号通信システムであって、暗号通信時の暗号処理を、CPUを用いて行う第1の通信装置と、別の第2の通信装置との間で、暗号通信を行い、前記暗号通信に用いる暗号アルゴリズムを、一方からの提案とその提案に対する応答通知という形で折衝するシステムであって、前記第1の通信装置は、暗号通信途中に、現在時点で使用している暗号アルゴリズムを通信相手と折衝

したときに、その折衝時点までの一定期間に測定したCPU使用率の平均値を記憶しておく折衝時CPU使用率記憶手段と、前記現在時点までの一定期間に測定したCPU使用率の平均値を求める手段と、前記折衝時CPU使用率記憶手段により記憶されたCPU使用率と現在時点でのCPUとが変化していることを検出する手段と、前記CPU使用率の変化検出したときに、請求項1～12のいずれかに記載のアルゴリズム選択方法を利用して、一つもしくは複数の暗号アルゴリズムを選択する手段と、選択した前記暗号アルゴリズムが、既に使用している暗号アルゴリズムと異なれば、前記暗号アルゴリズムを通信相手に提案する手段とを含むことを特徴とする。

【0042】

上記請求項17の発明によれば、暗号通信途中において、前記第1の通信装置は、CPU使用率が変化した場合に、CPUリソースの不足によって前記第1の通信装置で動作するアプリケーションの実行に支障が出ることを防ぐことができるような暗号アルゴリズムを提案することにより、折衝を開始することができる。

【0043】

請求項18の発明は、暗号通信システムであって、暗号通信時の暗号処理を、CPUを用いて行う第1の通信装置と、別の第2の通信装置との間で暗号通信を行い、また一つの暗号通信において同時に複数の暗号アルゴリズムを使用可能であるシステムであって、前記第1の通信装置は、暗号処理が必要な通信データ送信時に、使用可能な複数の暗号アルゴリズムから、請求項1～14のいずれかに記載のアルゴリズム選択方法を利用して、一つの暗号アルゴリズムを選択する手段と、選択した前記暗号アルゴリズムを用いて前記送信データに暗号処理を施す手段とを含むことを特徴とする。

【0044】

上記請求項18の発明により選択された暗号アルゴリズムを用いて、暗号通信を行えば、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。さらに、使用する暗号アルゴリズムを変更するときに、暗号アルゴリズムを折衝し直す必要がないため、

より柔軟にCPU負荷を制御することができる。

【0045】

請求項19の発明は、暗号通信システムであって、暗号通信時の暗号処理を、CPUを用いて行う第1の通信装置と、別の第2の通信装置との間で暗号通信を行い、また一つの暗号通信において同時に複数の暗号アルゴリズムを使用可能であるシステムであって、前記第1の通信装置は、使用可能な複数の暗号アルゴリズムから、請求項1～14のいずれかに記載のアルゴリズム選択方法を利用して、一つの暗号アルゴリズムを選択する手段と、選択した前記暗号アルゴリズムを、前記第2の通信装置に通知する手段とを含み、前記第2の通信装置は、通知された前記暗号アルゴリズムを用いて前記送信データに暗号処理を施す手段を含むことを特徴とする。

【0046】

上記請求項19の発明により選択された暗号アルゴリズムを用いて、暗号通信を行えば、CPUリソースの不足によって、前記システム上で動作するアプリケーションの実行に支障が出ることを防ぐことができる。さらに、使用する暗号アルゴリズムを変更するときに、暗号アルゴリズムを折衝し直す必要がないため、より柔軟にCPU負荷を制御することができる。

【0047】

【発明の実施の形態】

以下、本発明の実施の形態を、図面を参照して説明する。

【0048】

（実施の形態1）

図1は、本発明の実施の形態1に関わるシステムの構成図である。図1を参照すると、実施の形態1のシステムは、放送設備100と、通信機能付き録画機能付き家電機器200と、ネットワークカメラ300と、インターネット400と、ディスプレイ（映像表示装置）500から構成される。

【0049】

次に、ネットワークカメラ300および、通信機能付き録画機能付き家電機器200の持つ機能を詳細に述べる。ネットワークカメラ300は、撮影機能部3

01と、暗号処理機能部302と、暗号アルゴリズムネゴシエーション機能部303と、通信機能部304とを具備する。

【0050】

また、通信機能付き録画機能付き家電機器200は、受像機能部201と、録画機能部202と、リソース監視機能部203と、暗号アルゴリズムネゴシエーション機能部204と、通信機能部205と、暗号処理機能部206とを具備する。なお、録画機能部202、リソース監視機能部203、暗号アルゴリズムネゴシエーション機能部204、通信機能部205、暗号処理機能部206はソフトウェアにより実現されており、これらの処理は内蔵CPUを利用して実行される。なお、本発明の方法は、本実施の形態においては、通信機能付き録画機能付き家電機器200内の暗号アルゴリズムネゴシエーション機能部204において用いられるものとして説明する。

【0051】

次に、システムの動作について説明する。

【0052】

まず、TV録画を行う際のシステムの動作について説明する。受像機能部201は放送設備100が放送しているTV放送データを受信する。続いて、受信されたTV放送データを、録画機能部202が内蔵の蓄積媒体に記録する。この処理は内蔵のCPUを利用して行われる。以上の処理を、録画したいTV番組の放送開始時刻から放送終了時刻まで連続的に行うことで、TV録画が完了する。

【0053】

次にネットワークカメラの映像をディスプレイに表示する際の、システムの動作について説明する。この処理は、暗号通信を行うための事前処理と、実際にネットワークカメラアプリケーションを動作させる処理の2つに分かれる。暗号通信を行うための事前処理については後述し、はじめに、実際にネットワークカメラアプリケーションを動作させる処理の概要について述べる。まず、ネットワークカメラ300では、撮影機能部301が撮影した映像データを、暗号処理機能部302が暗号化する。通信機能部304はその暗号化された映像データを、通信機能付き録画機能付き家電機器200宛のパケットとしてインターネット40

0に送出する。通信機能付き録画機能付き家電機器200では、通信機能部205でインターネットから暗号化パケットを受信し、暗号処理機能部206で復号化し、映像データをディスプレイ500に出力する。そして、ディスプレイ500が映像を表示する。以上のようにして、ネットワークカメラ300で撮影された映像がディスプレイ500に表示される。

【0054】

次に、暗号通信を行うための事前処理について説明する。ここでいう事前処理とは、ネットワークカメラ内の暗号アルゴリズムネゴシエーション機能部303と、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部204との間で、暗号通信に利用する暗号アルゴリズムおよび暗号化鍵、復号化鍵としてどのようなものを使用するかを折衝し、それぞれの暗号処理機能部302、206に設定する処理である。通信機能付き録画機能付き家電機器200の内蔵CPUが、図2に示したような、処理能力を超える事態を防止できるようにする折衝について、以下に説明してゆく。

【0055】

図19は、通信機能付き録画機能付き家電機器200が有する、ネゴシエーションに関わる部分を取り出したブロック図である。データ送信側とデータ受信側が同じ暗号アルゴリズムを使用するためには、双方の間で、ネゴシエーションが行われる。204は、暗号アルゴリズムネゴシエーション機能部である。通信機能部205は、相手の通信機能部との間で、データパケットの通信を行なう。暗号アルゴリズムのネゴシエーションにおいては、ネゴシエーション用のパケットを、相手との間でやり取りする。ネゴシエーションパケット作成・解釈部207は、送信時には、暗号アルゴリズム選択部209の指示に基づき、送信用のネゴシエーションパケットを所定の形式で作成し、受信時には、受信したネゴシエーションパケットの内容を解釈して暗号アルゴリズム選択部209に入手情報を渡す。また、暗号アルゴリズム選択部209は、決定した暗号アルゴリズムを暗号アルゴリズム設定部208に知らせて、アルゴリズム設定を指示する。暗号処理機能部206は、設定された暗号アルゴリズムを使用してデータの暗号化や復号化を行なう。暗号アルゴリズム選択部209は、リソース監視機能部203から

、あらかじめ、あるいは、ネゴシエーション時に入手したCPU使用率情報を格納するCPU使用率情報メモリ211を有している。本発明では、暗号アルゴリズム選択部209は、暗号アルゴリズムデータベース210や、リソース監視機能部203から得たCPU使用率情報を参照しながら、暗号アルゴリズムの提案処理や選択処理を行なう。暗号アルゴリズムデータベース210については、後述する。

【0056】

ここで、CPU使用率について説明する。CPU使用率は、CPUの処理能力を100%とした場合、TV録画アプリケーションやネットワークカメラアプリケーションなどの個々のアプリケーションが使用するCPU処理能力を%で表したものである。CPUの処理方式には種々の方式が存在するが、最も一般的なものは、ある時刻にタスクを一つだけ処理する方式である。複数のタスクを処理する場合は、それらのタスクを時分割で処理することにより、同時並行して処理しているように見せている。軽いタスクには、短い時間を、重いタスクには長い時間を割り当てる方法がある。また、時間を一定の短い処理時間単位（タイムスロット、スレッドなどと呼ぶ。）で区切り、重いタスクには軽いタスクよりも頻繁に単位時間を割り当てるようにする方法もある。CPUリソースに余裕があり、CPUがモニタプログラムなどの共通的处理を除いて、タスクを処理していない時間や処理時間単位は、アイドル状態として検出される。このようなCPU方式において、タスクのCPU使用率を計測するには、以下のようにすればよい。CPUのOS内のモニタプログラムなどを使用して、比較的短時間毎に、処理しているタスクが何であることをサンプリングして調べさせる。アプリケーションAがタスクAにより構成されている場合を考える。1000回調べた結果、500回がタスクAで、残りの500回は、CPUが待機状態、すなわちアイドル状態であったとする。この場合は、アプリケーションAのCPU使用率は、50%である。CPUは、OSのモニタ・プログラムなどの共通的カーネル処理を行なうが、この処理は全体から見ると少ないので、一応ここでは無視する。

【0057】

サンプル数は、ある程度多くして、その時刻の瞬間CPU使用率ではなく、あ

る程度平滑化されたCPU使用率、例えばその時刻までの一定時間の平均CPU使用率を計測して用いる。瞬間、あるいは、短時間のCPU使用率は、一時的に大きく変動するので、アプリケーションが必要とするCPU処理能力を算出するには適さない。

【0058】

アプリケーションAの処理が2つの部分に別れていて、タスクAとカーネル処理とにより実行される場合に、タスクAが500回、カーネル処理が100回、アイドル状態が400回と計測された場合は、アプリケーションAのCPU使用率は、60%となる。また、タスクAは50%、カーネル部分は10%と計測できる。つぎに、アプリケーションAとアプリケーションBの2つの処理プログラムが並行して実行される場合について説明する。アプリケーションBもその一部がカーネルにおいて処理されるものとする。カーネルにおいては、アプリケーションAとアプリケーションBの各一部が処理されるが、カーネル全体のCPU使用率しか計測できないことが多い。すなわち、カーネルの中で、どのようなアプリケーションが処理されているのか、また、共通カーネル処理が実行されているのか、などは、区別できないことが多い。従って、このケースでは、アプリケーションAとアプリケーションBのCPU使用率の合計値は、100%からアイドル処理のCPU使用率を差し引いたものとして計測できるものの、アプリケーションAとアプリケーションBの個々のCPU使用率は計測できない。なぜなら、カーネル処理の内のアプリケーションAとアプリケーションBの内訳が計測できないからである。もしも、アプリケーションAのみが実行されているときに、上記のように、アプリケーションAが60%、タスクAが50%、カーネル部分が10%と計測できていれば、引き算により、アプリケーションB、タスクB、カーネルのB部分を算出できる。

【0059】

つぎに、暗号アルゴリズムネゴシエーション処理について以下で詳細に述べる。以下では、ネットワークカメラ300および通信機能付き録画機能付き家電機器200内の、各暗号アルゴリズムネゴシエーション機能部303および204のうち、ネゴシエーションを開始する側をイニシエータ、イニシエータに対して

応答する側をレスポンドと呼ぶ。

【0060】

図3は暗号アルゴリズムネゴシエーションのシーケンスを表している。図3ではまず、イニシエータはレスポンドに対して、複数の暗号アルゴリズム（暗号アルゴリズム a、b、c）の情報を含んだ提案パケットをレスポンドに対して送信する。レスポンドはその提案パケットを受信すると、その中からひとつの暗号アルゴリズム（暗号アルゴリズム b）を選択し、イニシエータに対して、選択した暗号アルゴリズムの情報を含んだ応答パケットを送信する。イニシエータでは、レスポンドからの応答パケットを受信すると、そこに含まれている暗号アルゴリズム（暗号アルゴリズム b）を採用する。以上のようにして、イニシエータ、レスポンドの両方で、同じ暗号アルゴリズム（暗号アルゴリズム b）を使うことが約束され、暗号通信を行えるようになる。

【0061】

なお、イニシエータが提案する暗号アルゴリズムは1つでもよい。また、レスポンドは提案された暗号アルゴリズムに利用可能な暗号アルゴリズムがなければ、応答しなくてもよい。また、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部204が、イニシエータとして暗号アルゴリズムを提案したり、レスポンドとして暗号アルゴリズムを選択する際には、リソース監視機能部203から得たCPU使用率の情報をを用いるが、その際の具体的な手順については後述する。

【0062】

なお、暗号アルゴリズムを折衝する際のメッセージは、図3のシーケンスに限定するものではなく、既存の鍵交換プロトコルの規定に則って行っても良い。例えば、一般的にIPsecと併用されることが多い鍵交換プロトコルIKE（Internet Key Exchange）を使って、規定のメッセージシーケンスの中で暗号アルゴリズムを折衝しても良い。

【0063】

また、暗号アルゴリズムのネゴシエーションは、暗号通信を行う前に一度だけ行う動作を説明したが、暗号通信の途中においても暗号アルゴリズムをネゴシエ

ーションし直してもよい。

【0 0 6 4】

次に、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部 2 0 4 が、イニシエータとして、提案する暗号アルゴリズムを決定する手順や、レスポндаとして、イニシエータから提案された複数の暗号アルゴリズムの中から応答通知する暗号アルゴリズムを選択する手順について説明する。ところで、暗号アルゴリズムにはさまざまなものがあるが、それぞれによって暗号化復号化処理の負荷や、暗号の破られにくさを示す暗号強度が異なる。したがって、基本的には、ネットワークカメラ映像の暗号化に用いる暗号アルゴリズムは、CPU に余裕のある場合には、できるだけ暗号強度の高いものを選択してセキュリティを高め、CPU に余裕のない場合には CPU リソースが不足しないように、処理負荷の低いものを選択する。

【0 0 6 5】

＜通信機能付き録画機能付き家電機器がレスポндаとなる場合＞

さて、図 4、5 は、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部 2 0 4 がレスポндаとなる場合のフローチャートである。以下では、まず図 4 のフローチャートに沿って説明を行う。

【0 0 6 6】

まず、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部 2 0 4（以下レスポнда）は、暗号処理機能部 2 0 6 がサポートしている暗号アルゴリズムの集合 A を求める（ステップ 4 0 1）。ここで、ネットワークカメラ内の暗号アルゴリズムネゴシエーション機能部（以下イニシエータ）からの提案パケットを待つ状態になる。

【0 0 6 7】

次に、イニシエータは何らかのネゴシエーション開始要求を待つ状態になっているので、暗号通信を開始する際や、前回のネゴシエーションから一定時間経過後に自動で再ネゴシエーションを行なう場合、もしくは、何らかの理由でネゴシエーション開始コマンドを実行したときなどに発行される、ネゴシエーション開始要求を受けると（ステップ 4 1 1）、ネゴシエーションを開始する。すなわち

、1つもしくは複数の暗号アルゴリズムの提案を含むパケットをレスポンドに送信する（ステップ412）。この提案パケットを受信したレスポンドでは、提案されたアルゴリズムの集合Bをパケットから読み取る（ステップ402）。応答可能な暗号アルゴリズム（集合C）は、提案された暗号アルゴリズム（集合B）のうち暗号処理機能部206がサポートしているもの（集合A）であるので、 $C = A \cap B$ として求められる（ステップ403）。

【0068】

さて、ここからレスポンドに対して応答する暗号アルゴリズムを選択するステップに入る（ステップ500）。ステップ500の詳細は、図5のフローチャートを用いて説明する。

【0069】

ここでの前提としては、CPUを利用するアプリケーションは、TV録画とネットワークカメラのみとする。またこの時点では、TV録画機能だけがすでにCPUを利用しており、ネットワークカメラアプリケーションはまだ起動されておらず、CPUを利用していないとする。

【0070】

まず、リソース監視機能部203からCPU使用率CPUUtilを取得する（ステップ501）。CPUUtilは、その時点で実行されているアプリケーション（複数の場合は、合計）によるCPU使用率を表す。ただし、既に述べたように、リソース監視機能部203が、暗号アルゴリズムネゴシエーション機能部に対して通知するCPU使用率には、その時刻の瞬間CPU使用率ではなく、ある程度平滑化されたCPU使用率、例えばその時刻までの一定時間の平均CPU使用率等、を用いる。この理由は、瞬間CPU使用率を利用すると、CPU使用率の一時的な変動の影響を大きく受けるため、一定時間利用する暗号アルゴリズムを選択する適切な判断基準とはなりえないからである。

【0071】

次に、応答可能な暗号アルゴリズムの集合Cのなかで、以下の式（式1）を満たす暗号アルゴリズムの集合Dを求める（ステップ502）。

【0072】

$$\text{CPURecord} + \text{CPUCamera}(x) \leq \alpha \quad \cdots \text{(式1)}$$

ここで、 CPURecord はTV録画機能が消費するCPUリソース、 CPUCamera は暗号アルゴリズム x を用いて暗号通信を行ったときに、ネットワークカメラアプリケーションが必要とするCPUリソースである。したがって、(式1)が満たされるということは、TV録画と、暗号アルゴリズム x による暗号通信を同時に行っても、平均CPU使用率が α [%] 以下となり、両方のタスクが正常に実行されることを意味している。 α の値は、例えば95%などの値をあらかじめ設定しておく。暗号アルゴリズムネゴシエーション機能部204は、リソース監視機能部203から、複数の暗号アルゴリズムの各々について、暗号処理を行ったときにシステム全体で必要となるCPUリソースを計算するのに必要な、CPU使用率を(ステップ501)において取得し、全処理負荷($\text{CPURecord} + \text{CPUCamera}(x)$)として推定する全処理負荷推定手順を(ステップ502)において実施している。また、(ステップ502)において、集合Dを求めるために、各々の暗号アルゴリズムについて、前記全処理負荷と、第一基準値である α とを比較する比較手順を実施している。

【0073】

図6は、集合Cの要素が暗号アルゴリズム a 、 b 、 c であった場合の例である。この場合、(式1)を満たす暗号アルゴリズム(集合D)は b と c である。

【0074】

CPURecord 、 $\text{CPUCamera}(x)$ の求め方は、先に述べたCPU使用率の考え方をを用いると、以下のとおりとなる。まず、この時点でCPUを利用しているのはTV録画機能だけであるので、 $\text{CPURecord} = \text{CPUUtil}$ となる。また、 $\text{CPUCamera}(x)$ は、 $\text{CPUCamera}(x) = \text{CPUCameraConst} + \text{CPUCameraEnc}(x)$ として求められる。ここで、 CPUCameraConst は、暗号処理以外の処理でネットワークカメラアプリケーションが消費するCPUリソースであり、 $\text{CPUCameraEnc}(x)$ は暗号アルゴリズム x を用いたときに、暗号処理で消費するCPUリソースである。

【0075】

$CPU Camera Enc(x)$ は、アプリケーション層での通信速度に比例すると仮定すると、以下のようにして求められる。 $CPU Camera Enc(x) = (Camera Rate / Enc Rate(x)) \times 100 [\%]$ 。ここで、 $CPU Camera Rate$ は、ネットワークカメラアプリケーションが行う通信のアプリケーション層での通信速度、 $Enc Rate(x)$ は、暗号アルゴリズム x を利用した暗号通信処理のみに、内蔵の CPU を 100% 利用したときのアプリケーション層での通信速度である。

【0076】

ここで用いた、 $CPU Camera Const$ 、 $Camera Rate$ の値は、計測するのではなく、システムから与えられているものとする。また図 7 のような暗号アルゴリズムデータベース 210 を、図 19 に示したように、暗号アルゴリズムネゴシエーション部 204 に設けておく。暗号アルゴリズムデータベース 210 には、各暗号アルゴリズムの $Enc Rate(x)$ と共に、それぞれの暗号強度の順位が格納されている。暗号アルゴリズム x から $Enc Rate(x)$ を求めることができる。

【0077】

なお、ここではネットワークカメラアプリケーションは開始されていないとした場合について説明したが、既に開始されており、暗号アルゴリズムとして z が用いられていた場合には、 $CPU Record = CPU Util - CPU Camera(z)$ のように、TV 録画機能に必要な CPU リソースを求めることができる。また、 $CPU Record$ の値がシステムから与えられている場合には、その値を用いることもできる。また $CPU Record$ を、以前にこの CPU 上で TV 録画機能のみが実行されていた期間の平均 CPU 使用率としてもよい。また、 $CPU Camera(x)$ を、以前にこの CPU 上で暗号アルゴリズム x を用いたネットワークカメラアプリケーションのみが実行されていた期間の平均 CPU 使用率としてもよい。これらの CPU 使用率情報を、図 19 の CPU 使用率情報メモリ 211 に格納しておく。

【0078】

次に、集合 D が空集合かどうか、すなわち (式 1) を満たす暗号アルゴリズム

が存在するかどうかを判定する（ステップ503）。空集合の場合、つまり（式1）を満たす暗号アルゴリズムが存在しない場合は、どの暗号アルゴリズムを用いても、CPUリソースが不足することを示しているため、できるだけCPU処理負荷を軽減するために、応答可能な暗号アルゴリズム（集合C）のうち最も処理負荷の低いものを選択する（ステップ505）。

【0079】

集合Dが空集合でない場合は、その中で最も暗号強度の高い暗号アルゴリズムを選択する（ステップ504）。図6の例では、集合Dに含まれるb、cのうち暗号強度の高いbが選ばれる。暗号アルゴリズムの処理負荷や、暗号強度の情報は図7の暗号アルゴリズムデータベースから得ることができる。（ステップ503）と（ステップ504）においては、前記全処理負荷が前記第一基準値を下回る、ひとつもしくは複数の暗号アルゴリズムを選択する選択手順を実施していることになる。

【0080】

なお、ここでは集合Dが空集合の場合に、集合Cのうち最も処理負荷の低い暗号アルゴリズムを応答通知したが、CPUの処理能力を超える場合があるので、TV録画機能を優先する場合には、応答パケットをイニシエータに送信せずに、ネットワークカメラアプリケーションを開始しない、もしくは既に開始している場合には中断することもできる。また、カメラ映像を間引いて画質を落として伝送するようにしてもよい。

【0081】

以降は再び図4を用いて説明する。暗号アルゴリズムを選択したら、選択した暗号アルゴリズムの情報を含む応答パケットをイニシエータに対して送信する（ステップ404）。

【0082】

次に、応答通知した暗号アルゴリズムを実際に利用するために、暗号処理機能部にその暗号アルゴリズムを設定する（ステップ405）。一方、レスポндаでは、イニシエータからの応答パケットを受信し（ステップ413）、応答通知された暗号アルゴリズムをネットワークカメラ内の暗号処理機能部302に設定す

る（ステップ414）。

【0083】

このあと、ネットワークカメラ300は、撮影機能部301で撮像した映像データを、暗号処理機能部302において、設定された暗号アルゴリズムの暗号化機能を使用して暗号化データとし、暗号アルゴリズムネゴシエーション部303に設定された暗号アルゴリズムの識別子、または、暗号アルゴリズムと鍵とを特定するセキュリティアソシエーションと呼ばれる情報SAの識別IDを添付する。そして、通信機能部304において、インターネット400に送出する。通信機能付き録画機能付き家電機器200の通信機能部205は、パケットを受信し、添付された暗号アルゴリズムの識別子、または、SAの識別IDをもとに、折衝、合意した暗号アルゴリズムを使用して、暗号処理機能部206において、暗号の復号化を行ない、映像データをディスプレイ500に表示する。

【0084】

＜通信機能付き録画機能付き家電機器がイニシエータとなる場合＞

次に、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部204がイニシエータとなり、ネットワークカメラ内の暗号アルゴリズムネゴシエーション機能部303とネゴシエーションを行う場合の手順を示す。また、図8、9はこのときの動作手順を示すフローチャートである。以下では、まず、図8のフローチャートに沿って説明を行う。

【0085】

まず、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部204（以下イニシエータ）は、暗号処理機能部206がサポートしている暗号アルゴリズムの集合Aを求める（ステップ801）。ここで、何らかのネゴシエーション開始要求を待つ状態になる。ネゴシエーションの開始要求は、暗号通信を開始する際や、前回のネゴシエーションから一定時間経過後、もしくは、ネゴシエーション開始コマンドを実行したときなどに発行される。

【0086】

イニシエータは、ネゴシエーションの開始要求を受け付けると（ステップ802）、CPU使用率を用いて暗号アルゴリズムを選択する（ステップ900）。

ステップ900の詳細な手順は（図9のステップ901～905）、通信機能付き録画機能付き家電機器がレスポンドの場合（図4のステップ500、すなわち図5）とほぼ同じであるので、ここでは省略する。異なるのは、暗号アルゴリズムを選択する集合が、応答通知可能な暗号アルゴリズム（集合C）か、サポートしている暗号アルゴリズム（集合A）かの違いのみである。

【0087】

次に、選択した暗号アルゴリズムをレスポンドに対して提案する（ステップ804）。

【0088】

レスポンドでは、はじめに暗号処理機能部302がサポートしている暗号アルゴリズムの集合Eを求めておく（ステップ811）。その後、イニシエータから提案パケットを受信すると（ステップ812）、提案されたアルゴリズムをサポートしているか（集合Eに含まれているか）を判断する（ステップ813）。提案された暗号アルゴリズムをサポートしていない（集合Eに含まれていない）場合は、イニシエータに応答を返すことができないので、ネゴシエーションに失敗し、次の提案パケットを待つ。提案された暗号アルゴリズムをサポートしている（集合Eに含まれている）場合には、その暗号アルゴリズムをイニシエータに対して応答し（ステップ814）、応答通知した暗号アルゴリズムを暗号処理機能部302に設定する（ステップ815）。

【0089】

イニシエータでは、応答パケットを受信すると（ステップ804）、応答通知された暗号アルゴリズムを暗号処理機能部206に設定する（ステップ805）。

【0090】

以上のように、イニシエータに対して応答通知する、もしくはレスポンドに対して提案する暗号アルゴリズムを選択する際に、CPUリソースが不足しない範囲で、暗号強度の最も高いものを選択することによって、できるだけ強固なセキュリティを保ちつつ、ネットワークカメラのような暗号通信を必要とするアプリケーションと、TV録画のようなその他の処理を並行して行ったときの、CPU

リソースの不足を防ぐことができる。

【0091】

なお、ここではレスポンドに対して提案する暗号アルゴリズムは1つであるとしたが、優先順位を低くしておけば、他の暗号アルゴリズムを複数提案してもよい。

【0092】

また、ここではネットワークカメラ以外のアプリケーションは、TV録画のみとしていたが、TV録画以外の他のアプリケーションが存在した場合には、上述の「CPURecord」を、「暗号アルゴリズムネゴシエーションの対象となる暗号通信以外の、全てのアプリケーションが使用するCPU使用率の合計」として読み替えることで、同様の処理が可能である。

【0093】

また、TV録画に必要なCPUリソースCPURecordをCPU利用率CPUUtilから計算したが、CPUUtilが α [%] を越えていた場合には、上記の方法ではCPURecordを小さく見積もっていることになる。この場合、ステップ502、902で選択した暗号アルゴリズムを用いて暗号通信を行っても、CPU利用率が α [%] を越えてしまう可能性がある。以上のような問題を回避するために、ステップ501、901で取得したCPU使用率が α [%] を越えていた場合には、集合C（レスポンドの場合）もしくは、集合A（イニシエータの場合）のうち最も処理負荷の低い暗号アルゴリズムを選択してもよい。

【0094】

CPUUtilが α [%] を越えているとは、CPUUtilを計測したときに、TV録画機能に必要なCPUリソースを確保できていないことを意味する。具体的な例で説明する。TV録画をするのに必要なCPUリソースであるCPURecordが80%であるとする。また、暗号アルゴリズム z を利用した場合には、ネットワークカメラアプリケーションが必要とするCPUリソースであるCPUCamera(z)が40%であったとする。 $\alpha = 95\%$ とする。TV録画とネットワークカメラアプリケーション（暗号含む）を実行している場合、必要

なCPUリソースは、 $80\% + 40\% = 120\%$ となるが、CPU使用率が100%を超えることはないので、CPU使用率の計測値CPUUtilは、このとき、100%に近い値 ($\alpha = 95\%$ を越える値、例えば98%) として計測される。このとき、TV録画やネットワークカメラアプリケーションは正常に動作できていない状態にある。このような状態で計測したCPUUtilをもとにCPURecordを計算すると、 $CPURecord = CPUUtil - CPUCamera(z)$ は、 $98\% - 40\% = 56\%$ となる。80%であるべきところを56%と計算してしまう。すなわち、小さく見積もることになる。ここで、 $CPUCamera(y) = 30\%$ となる暗号アルゴリズムが存在した場合、 $CPURecord + CPUCamera(y) = 56\% + 30\% = 86\% < 95\%$ (α) となり、暗号アルゴリズムyを選択することができる。しかし、本当にTV録画をするのに必要なCPUリソース80%であるので、TV録画およびネットワークカメラアプリケーションを実行するのに本当に必要なCPUリソースは、 $80\% + 30\% = 110\% > \alpha$ となってしまう、やはり正常に動作することができない。いいかえると、 $CPUUtil > \alpha$ と計測された場合は、その時、実行しているアプリケーションに対して、十分なCPUリソースが割り当てられているとは限らないということになる。このように、 $CPUUtil > \alpha$ と判定され、正常な動作ができていない場合、本当のCPURecordを求めることができず、適切な暗号アルゴリズムを選択ができないので、暗号アルゴリズムを変更した後に正常な動作をする可能性が比較的高い、最も処理負荷の低い暗号アルゴリズムを選択してもよいのである。もちろん、最も処理負荷の低い暗号アルゴリズムを選択したからといって、正常に動作するようになるという保証は、必ずしもないので、その場合は、異常動作を報告するモードに移るようにしてもよい。このモードにおいて、不要不急のアプリケーションの処理を、一時停止するか処理速度を遅くして、必要なCPUリソースを確保するなどの処理を行えばよい。

【0095】

(実施の形態2)

次に実施の形態2について説明する。全体のシステム構成など、実施の形態1

と変わらない部分の説明は、ここでは省略する。実施の形態 1 と異なるのは、暗号アルゴリズムを選択する手順のみであるので、その部分について以下で説明する。

【0096】

実施の形態 2 では、実施の形態 1 と違い、ネットワークカメラアプリケーションを実行するのに必要な CPU リソースが分からない場合にでも適用できる方法を説明する。

【0097】

＜通信機能付き録画機能付き家電機器がレスポンドとなる場合＞

図 10、11 は、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部 204 がレスポンドとなる場合のフローチャートである。以下では、まず 10 図のフローチャートに沿って説明を行う。

【0098】

まず、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部 204（以下レスポンド）は、暗号処理機能部 206 がサポートしている暗号アルゴリズムの集合 A を求める（ステップ 1001）。こうして、ネットワークカメラ内の暗号アルゴリズムネゴシエーション機能部（以下イニシエータ）からの提案パケットを待つ状態になる。

【0099】

次に、イニシエータは暗号アルゴリズムネゴシエーションの開始要求を受け付け（ステップ 1011）、ネゴシエーションを開始する。すなわち、1 つもしくは複数の暗号アルゴリズムの提案を含むパケットをレスポンドに送信する（ステップ 1012）。この提案パケットを受信したレスポンドでは、提案されたアルゴリズムの集合 B をパケットから読み取る（ステップ 1002）。応答通知可能な暗号アルゴリズム（集合 C）は、提案された暗号アルゴリズム（集合 B）のうち暗号処理機能部 206 がサポートしているもの（集合 A）であるので、 $C = A \cap B$ として求められる（ステップ 1003）。

【0100】

次に、集合 C から暗号アルゴリズムを選択する（1100）。ステップ 110

0の詳細は、図11のフローチャートを用いて説明する。

【0101】

まず、この暗号アルゴリズムネゴシエーションが暗号通信開始前かどうかを判断する（ステップ1104）。暗号通信開始前の場合は、暗号強度よりもCPU負荷を軽減することを優先して、集合Cのうち最も処理負荷の低い暗号アルゴリズムを応答通知する（ステップ1102）。

【0102】

暗号通信を既に開始している場合には、そのときのCPU使用率に応じて、応答通知する暗号アルゴリズムを切り替える。まず、リソース監視機能部からその状態での、すなわち、使用中の暗号アルゴリズムなどを含めたCPU使用率CPU Utilを取得する（ステップ1103）。次に、暗号アルゴリズムを切り替える際の閾値として、2つの値 γ [%] と δ [%] ($\gamma \geq \delta$) を用いる。 γ 、 δ の値は例えば90 [%]、70 [%] などとあらかじめ決めておく。すなわち、 $\delta < \text{CPU Util} < \gamma$ の場合には、CPU使用率が高すぎず低すぎず適当であると判断し、現在使用している暗号アルゴリズムを選択する（ステップ1104、1108、1107）。

【0103】

$\text{CPU Util} \geq \gamma$ の場合（ステップ1104）は、CPU負荷が高すぎると判断して、現在使用している暗号アルゴリズムよりもCPU負荷が低い暗号アルゴリズムを選択する。ただし、できるだけ強固な暗号アルゴリズムを使用するために、現在使用している暗号アルゴリズムよりもCPU負荷が低い暗号アルゴリズムの中でも、最も暗号強度の高いものを選択する（ステップ1105、1106）。現在使用している暗号アルゴリズムが既に、集合Cのうち最も負荷の低いものだった場合には、その暗号アルゴリズムを選択する（ステップ1105、1107）。

【0104】

$\text{CPU Util} \leq \delta$ の場合（ステップ1104、1108）は、CPUリソースに余裕があると判断し、現在使用している暗号アルゴリズムよりも、より暗号強度の高い暗号アルゴリズムを選択する（ステップ1109、1110）。ただ

し、CPU 負荷が突然高くなるのを防ぐため、現在使用している暗号アルゴリズムよりも暗号強度が高い暗号アルゴリズムの中でも、最も処理負荷の低い暗号アルゴリズムを選択する。現在使用している暗号アルゴリズムが既に、集合 C のうち最も暗号強度の高いものだった場合には、その暗号アルゴリズムを選択する（ステップ 1109、1107）。

【0105】

（ステップ 1103）においては、暗号処理実行中の任意の時刻に、その時点までの一定期間に測定した CPU 使用率の平均値を求める手順により、あらかじめ、CPU 使用率 CPU_{util} が求められているものとする。また、このステップにおいて、CPU 使用率 CPU_{util} を求めるようにしてもよい。（ステップ 1104）は、前記 CPU 使用率と第二基準値 γ とを比較する手順を実施している。（ステップ 1105）と（ステップ 1105）は、比較の結果前記 CPU 使用率が第二基準値よりも高い場合は、その時点で使用している暗号アルゴリズムよりも、負荷の低い一つもしくは複数の暗号アルゴリズムを選択する手順を実施している。

【0106】

（ステップ 1105）、（ステップ 1106）、（ステップ 1110）では、暗号アルゴリズムの暗号強度の比較や、最も高いものの選択を行なうが、このために、これらのステップの前、または、その中で、暗号強度の順序を求める手順を実行する。図 7 の暗号アルゴリズムデータベースには、各暗号アルゴリズムの $EncRate(x)$ と共に、それぞれの暗号強度の順位が格納されている。暗号強度の比較や、最も高いものの選択のため、各暗号アルゴリズムについて、その暗号強度データを読み出し、比較することにより、暗号強度の順序を知ることができる。

【0107】

（ステップ 1108）は、前記 CPU 使用率と第三基準値 δ とを比較する手順である。（ステップ 1109）、（ステップ 1110）は、前記 CPU 使用率が第三基準値よりも低い場合において、その時点で使用している暗号アルゴリズムよりも、暗号強度の高い一つもしくは複数の暗号アルゴリズムを選択する手順を

実施している。

【0108】

(ステップ1104)と(ステップ1105)で、前記CPU使用率と第二基準値 γ および第三基準値 δ とを比較し、前記CPU使用率が第二基準値 γ より低く第三基準値 δ より高い場合は、(ステップ1107)において、その時点で使用している暗号アルゴリズムを選択する手順を実施することになる。

【0109】

以降は再び、図10に戻って説明する。まず、選択した暗号アルゴリズムをイニシエータに対して応答通知する(ステップ1004)。

【0110】

次に、応答通知した暗号アルゴリズムを実際に利用するために、暗号処理機能部にその暗号アルゴリズムを設定する(ステップ1005)。一方、レスポндаでは、イニシエータからの応答パケットを受信し(ステップ1013)、応答通知された暗号アルゴリズムをネットワークカメラ内の暗号処理機能部302に設定する(ステップ1014)。

【0111】

<通信機能付き録画機能付き家電機器がイニシエータとなる場合>

次に、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部204がイニシエータとなり、ネットワークカメラ内の暗号アルゴリズムネゴシエーション機能部303とネゴシエーションを行う場合の手順を示す。また、図12、13はこのときの動作手順を示すフローチャートである。以下では、まず図12のフローチャートに沿って説明を行う。

【0112】

まず、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部204(以下イニシエータ)は、暗号処理機能部206がサポートしている暗号アルゴリズムの集合Aを求める(ステップ1201)。ここで、何らかのネゴシエーション開始要求を待つ状態になる。ネゴシエーションの開始要求は、暗号通信を開始する際や、前回のネゴシエーションから一定時間経過後、もしくは、ネゴシエーション開始コマンドを実行したときなどに発行される。

【0113】

イニシエータは、ネゴシエーションの開始要求を受け付けると（ステップ1202）、CPU使用率を用いて暗号アルゴリズムを選択するが、その手順（ステップ1300、詳細は図13）は、通信機能付き録画機能付き家電機器がレスポンドの場合（図10のステップ1100、詳細は図11）とほぼ同じであるので、ここでは省略する。異なるのは、暗号アルゴリズムを選択する集合が、応答通知可能な暗号アルゴリズム（集合A）か、サポートしている暗号アルゴリズム（集合C）かの違いのみである。

【0114】

そして、選択した暗号アルゴリズムをレスポンドに対して提案する（ステップ1203）。

【0115】

レスポンドでは、はじめに暗号処理機能部302サポートしている暗号アルゴリズムの集合Eを求めておく（ステップ1211）。その後、イニシエータから提案パケットを受信すると（ステップ1212）、提案されたアルゴリズムをサポートしているか（集合Eに含まれているか）を判断する（ステップ1213）。提案された暗号アルゴリズムをサポートしていない（集合Eに含まれていない）場合は、イニシエータに応答を返すことができないので、ネゴシエーションに失敗し、次の提案パケットを待つ。提案された暗号アルゴリズムをサポートしている（集合Eに含まれている）場合には、その暗号アルゴリズムをイニシエータに対して応答通知し（ステップ1214）、応答通知した暗号アルゴリズムを暗号処理機能部302に設定する（ステップ1215）。

【0116】

イニシエータでは、応答パケットを受信すると（ステップ1204）、応答通知された暗号アルゴリズムを暗号処理機能部206に設定する（ステップ1205）。

【0117】

以上のように、イニシエータに対して応答通知する、もしくはレスポンドに対して提案する暗号アルゴリズムを選択する際に、CPU使用率に応じてより適切

な暗号アルゴリズムに切り替えていくことによって、できるだけ強固なセキュリティを保ちつつ、ネットワークカメラのような暗号通信を必要とするアプリケーションと、TV録画のようなその他の処理を並行して行ったときの、CPUリソースの不足を防ぐことができる。

【0118】

なお、ここではレスポндаに対して提案する暗号アルゴリズムは1つであるとしたが、優先順位を低くしておけば、他の暗号アルゴリズムを複数提案してもよい。

【0119】

また、ここでは、暗号アルゴリズムのネゴシエーションについて説明したが、認証アルゴリズムのネゴシエーションの場合にも適用できる。

【0120】

(実施の形態3)

次に実施の形態3について説明する。全体のシステム構成など、実施の形態1と変わらない部分の説明は、ここでは省略する。実施の形態1と異なるのは、暗号アルゴリズムのネゴシエーションを行うタイミングと、暗号アルゴリズムを選択する手順のみであるので、その部分について以下で説明する。

【0121】

実施の形態3では、定期的にCPU使用率の変化を検知し、あらかじめ定められたタイミングではなく、CPU使用率が変化したタイミングで、通信機能付き録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部204がイニシエータとなり、ネットワークカメラ内の暗号アルゴリズムネゴシエーション機能部303とネゴシエーションを行う場合の手順を示す。

【0122】

また、図14、15は実施の形態3の動作手順を示すフローチャートである。以下では、まず図14のフローチャートに沿って説明を行う。

【0123】

まず、それぞれの暗号アルゴリズムネゴシエーション機能部204、303で、サポートしている暗号アルゴリズムの集合A、Eを求める(ステップ1401

、1421)。

【0124】

次に、暗号通信開始前に、それぞれの暗号アルゴリズムネゴシエーション機能部204、303の間で、実施の形態1の手順に従って、暗号アルゴリズムのネゴシエーションを行う(ステップ1402、1422)。そして、このネゴシエーションに従って選択された暗号アルゴリズムを用いて暗号通信が開始される。このとき、この時点でのCPU使用率を $preCPUUtil$ として保持しておく。なお、ここではどちらがイニシエータとなってネゴシエーションを行ってもよい。

【0125】

さて、その後暗号通信を継続する間、定期的にはリソース監視機能部からCPU使用率 $CPUUtil$ を取得する(ステップ1403)。そして、前回ネゴシエーション時のCPU使用率 $preCPUUtil$ との差分 $CPUdiff$ を次のように計算する。 $CPUdiff = CPUUtil - preCPUUtil$ 。

【0126】

ここで、 $CPUUtil$ と $preCPUUtil$ との差が、ある一定値 β [%]よりも大きいかどうかを次の不等式が成り立つどうかで判定する(ステップ1404)。なお、 β の値は、例えば5%のようにあらかじめ定めておく。 $|CPUdiff| \geq \beta$ 。この式が成り立たないとき、つまり前回のネゴシエーション時に比べて、CPU使用率の変化が β [%]未満である場合は、暗号アルゴリズムを変更する必要はないと判断し、ネゴシエーションを行わない。

【0127】

上記の不等式が成り立つとき、つまり、前回のネゴシエーション時に比べて、CPU使用率の変化が β [%]以上であるときは、暗号アルゴリズムを変更する必要があるかもしれないと判断し、使用すべき暗号アルゴリズムを求める。その結果、暗号アルゴリズムを変更する必要がある場合は、イニシエータとして、提案パケットをレスポндаに対して送信する。ここでの手順(ステップ1500、1405)は、実施の形態1の、通信機能付き録画機能付き家電機器がイニシエータの場合(図8のステップ900、803)とほぼ同じであるので、ここで

は省略する。異なるのは、提案パケットを必ず送信するのか、暗号アルゴリズムが変更となるときにだけ送信するのか、のみである。

【0128】

次に、レスポンドは受信した提案パケットに対して、応答パケットを送信し、応答通知した暗号アルゴリズムを暗号処理機能部に設定する。また、イニシエータは応答パケットを受信すると、応答通知された暗号アルゴリズムを暗号処理機能部に設定する。以上の手順（ステップ1406、1407、1423～1426）は、実施の形態1の、通信機能付き録画機能付き家電機器がイニシエータの場合（図8のステップ804、805、812～815）と全く同じであるので、詳細は省略する。

【0129】

最後に、次のステップ1403で、CPU使用率の変化を計算するために、ここでのCPU使用率CPUUtilの値をpreCPUUtilに設定する（ステップ1408）。

【0130】

以上のように、CPU使用率に変化が起こったときに、新しい暗号アルゴリズムをネゴシエーションすることで、より柔軟に、できるだけ強固なセキュリティを保ちつつ、ネットワークカメラのような暗号通信を必要とするアプリケーションと、TV録画のようなその他の処理を並行して行ったときの、CPUリソースの不足を防ぐことができる。

【0131】

なおここでは β の値は一定値としているが、現在使用している暗号アルゴリズムや、その他の集合Aに含まれる暗号アルゴリズムが必要とするCPUリソース等に基づいて動的に変化させてもよい。たとえば、複数の暗号アルゴリズムの各CPU使用率間の差に比べて、 β 値が小さいと、その時のCPU使用率の変化が少しであっても、 β 値を超えるので、（ステップ1500）の選択判定を開始することになるが、暗号アルゴリズムを変更するほどのCPU使用率の余裕がないことが分かり、選択判定が無駄になる。選択中の暗号アルゴリズムとCPU使用率において隣接するアルゴリズムとのCPU使用率の差値を β 値とし、選択中の

暗号アルゴリズムによって β 値を動的に変えるようにすれば、無駄な処理を削減できる。

【0132】

(実施の形態4)

次に実施の形態4について説明する。全体のシステム構成など、実施の形態1と変わらない部分の説明は、ここでは省略する。実施の形態1と異なるのは、暗号アルゴリズムのネゴシエーションを行うタイミングと、暗号アルゴリズムを選択する手順のみであるので、その部分について以下で説明する。

【0133】

実施の形態4では、暗号アルゴリズムネゴシエーション時に複数の暗号アルゴリズムを合意しておく。そして、暗号化側でパケットを送信する際に、合意した暗号アルゴリズムのうち、どの暗号アルゴリズムを用いて送信パケットの暗号化を行っても、復号化側では正しく復号できるようにする。

【0134】

以下では、CPU使用率にもとづいて暗号アルゴリズムを選択し、その暗号アルゴリズムを用いて送信パケットを暗号化する手順と、選択した暗号アルゴリズムを通信相手に通知し、通信相手がその暗号アルゴリズムを用いて送信パケットを暗号化する手順を示す。

【0135】

図16、17は実施の形態4の動作手順を示すフローチャートである。図16の左側および図17は、CPU使用率に基づいて暗号アルゴリズムを選択する側の動作手順を、図16の右側は選択した暗号アルゴリズムを通知される側の動作手順を示している。以下では、まず図16のフローチャートに沿って説明を行う。

【0136】

<暗号アルゴリズム選択側の動作手順>

まず、暗号アルゴリズムネゴシエーションを行う(ステップ1601)。このとき、通信相手と複数の暗号アルゴリズムを合意し、その全ての暗号アルゴリズムの暗号化鍵、復号化鍵を生成しておく。ここで合意した暗号アルゴリズムの集

合を集合Fとする。

【0137】

次に、パケット送信要求が発生するまで待つ状態に入る（ステップ1602）。パケット送信要求が発生すると、CPU使用率から使用すべき暗号アルゴリズムを選択する（ステップ1700、詳細は図17）。なお、ここでのアルゴリズム選択方法は、実施の形態1におけるアルゴリズム選択方法（図4のステップ500、詳細は図5）とほぼ同じであるので、ここでは説明を省略する。実施の形態1におけるアルゴリズム選択方法と異なるのは、選択肢となる暗号アルゴリズムの集合が、集合Cであるか、集合Fであるかの違いのみである。

【0138】

なお、ここではパケット送信ごとに使用する暗号アルゴリズムを選択しているが、複数のパケット毎に、あるいは、一定時間おきに選択するようにしてもよい。

【0139】

次に、選択した暗号アルゴリズムを通信相手に通知するパケットを送信する（ステップ1603）。これは、通信相手が送信パケットを暗号化する際に使用すべき暗号アルゴリズムを、通信相手に通知することを目的としている。最後に、選択した暗号アルゴリズムで送信パケットを暗号化し送信して、パケット送信要求を受け付ける状態に入る（ステップ1604）。

【0140】

（ステップ1602）において受け付けるパケット送信要求は、ネットワークカメラ300や通信機能付き録画機能付き家電機器200に対する使用者の操作や、カメラ映像データを連続的に送信するなどの、アプリケーションの動作により起こるもの、IPレイヤなどでのプロトコルの動作により発生するもの、などがありうる。典型的な例は、ネットワークカメラの場合、ボタンを押すことによりカメラアプリケーションが動作し、「カメラアプリケーションが映像データパケット送信を要求する」である。また、同時に、通信制御用パケットや、暗号アルゴリズムネゴシエーションパケットなどを暗号化する場合もある。

【0141】

(ステップ1604)では、(ステップ1602)において送信を要求されたパケットを暗号化して送信する。また、(ステップ1603)において、ネットワークカメラが送信データを暗号化する際に使用すべき暗号アルゴリズムが通知されているので、ネットワークカメラ側では、これにもとづいて送信パケットを暗号化することができる。このステップは、図16のフローチャートの中で行なってもよいし、受信パケットの暗号解読のフローチャートにしたがって行なってもよい。

【0142】

(ステップ1603)は、ネットワークカメラ300が送信するデータを暗号化する際に用いる暗号アルゴリズムを、通信機能付き録画機能付き家電機器200がネットワークカメラ300に通知するためのステップである。

【0143】

(ステップ1604)は、通信機能付き録画機能付き家電機器200からネットワークカメラ300のための制御用パケットなどが、必要に応じて、ネットワークカメラ300に対して送信されるステップである。

【0144】

なお、(ステップ1604)で送信した暗号パケットを、ネットワークカメラ300において復号化する場合は、暗号パケットに付属するSA識別ID(SPI)を参照して、そのパケットがどの暗号アルゴリズムによって暗号化されているかを判別し、暗号の復号化を行なう。

【0145】

なお、制御用パケットなどを送信しないアプリケーションの場合には、(ステップ1700)、(ステップ1603)が、パケット送信要求(ステップ1602)によってではなく、一定時間ごとに実行されようにしてもよい。

【0146】

<暗号アルゴリズム被通知側の動作手順>

まず、暗号アルゴリズムネゴシエーションを行う(ステップ1621)。このとき、通信相手と複数の暗号アルゴリズムを合意し、その全ての暗号アルゴリズムの暗号化鍵、復号化鍵を生成しておく。また、パケット送信時に使用する暗号

アルゴリズムを設定する（ステップ1623）。なおステップ1623で設定する暗号アルゴリズムはステップ1621において、実施の形態1と同様の方法で選択される。

【0147】

次に、パケット送信要求が発生するまで待つ状態に入る（ステップ1624）。パケット送信が発生すると、ステップ1623で設定された暗号アルゴリズムを用いて送信パケットを暗号化し、送信する（ステップ1625）。

【0148】

ステップ1624でパケット送信が発生しなかった場合および、ステップ1625でパケット送信を完了したら、使用する暗号アルゴリズムの変更を通知するパケットを受信しているかをチェックする（ステップ1622）。受信していれば、使用する暗号アルゴリズムを設定し直し（ステップ1623）、パケット送信待ち状態に入る（ステップ1624）。受信していなければ、そのままパケット送信待ち状態に入る（ステップ1624）。

【0149】

なお、（ステップ1625）で送信したパケットを通信機能付き録画機能付き家電機器200が受信するには、（ステップ1604）と（ステップ1602）の間に、暗号化データのパケットを受信したかどうかの判断を行ない、受信した場合には、暗号解読を行なうステップを付け加えてもよい。また、このフローチャートの手順とは別に、暗号化データのパケット受信とその解読を行なう手順を、割り込みなどを契機に行なうように設けてよい。

【0150】

この実施の形態4においては、CPUリソースに余裕があった場合、通信機能付き録画機能付き家電機器200において、それまで使われていた暗号アルゴリズムよりも負荷の高い暗号アルゴリズムが選択され、ネットワークカメラ200に通知されたが、その直後に通信機能付き録画機能付き家電機器200においてCPU使用率が何らかの理由のために増加し、その直前にネットワークカメラ200で暗号アルゴリズムxによって暗号化されたカメラ映像パケットを、受信した通信機能付き録画機能付き家電機器200ではCPUリソースが不足している

ために復号化できない危険がある。このような危険を防止するために、暗号アルゴリズムを使用して通信している場合は、通信機能付き録画機能付き家電機器 200 において、CPUリソースの消費を増やすようなアプリケーションの追加や、変更を暗号通信が終わるまで禁止するか、その危険をOSやユーザに知らせて、適切な処理を行なう手順に入るようにすればよい。このような危険防止の処理は、本発明の各実施の形態においても適用できる。

【0151】

(その他の実施の形態)

上記説明した各実施の形態において、CPU使用率の各種推定手順は、その推定値が必要になったときに、リソース監視機能部 203 から入手する方法を中心に説明した。通信機能付き録画機能付き家電機器 200 が実行する可能性のある各種アプリケーションの中で、複数が同時並行して実行されるものは、あらかじめ分かっている場合が多い。そのようなアプリケーションについては、それぞれ予め実行してみて、リソース監視機能部 203 により CPU 使用率を計測し、計測した値を、既定の値として、CPU 使用率情報メモリ 211 に格納しておき、折衝時に取り出して使用するようにしてもよい。また、同じ組み合わせで実行される可能性のある 2 つ以上の複数のアプリケーションについて、予め試験的に実行してみたり、過去に同じ組み合わせで実行されている期間について、CPU 使用率を計測し、既定の値として、CPU 使用率情報メモリ 211 に格納しておき、折衝時に取り出して使用するようにしてもよい。また、通信機能付き録画機能付き家電機器 200 の設計時に、各種 CPU 使用率を算出し、既定の値として、CPU 使用率情報メモリ 211 に格納しておいてもよい。

【0152】

なお、CPU 使用率の仕組みと計測方法については、採用する CPU が適用している仕組みと計測方法に従えばよく、上記説明の例に限定されることはない。

【0153】

なお、上記各実施の形態においては、通信機能付き録画機能付き家電機器 200 におけるネゴシエーションについて説明したが、他の機器、装置においても、本発明を適用できる。また、相手機器も、本発明のネゴシエーションの仕組みを

有し、その機器内部でのCPU使用率に従って、適用可能な複数のアルゴリズムを選択しながら、両者間でネゴシエーションを行ない、最終的に使用するアルゴリズムを選択するようにしてもよい。

【0154】

なお、暗号アルゴリズムのように、同じ基本機能を有するが、処理能力や性能、および、CPU使用率に差異のある複数のアプリケーションプログラムから選択する状況にあれば、本発明を適用することができる。

【0155】

以上のように、送信パケットを暗号化する暗号アルゴリズムを選択する際に、CPUリソースが不足しない範囲で、暗号強度の最も高いものを選択することによって、より柔軟に、できるだけ強固なセキュリティを保ちつつ、ネットワークカメラのような暗号通信を必要とするアプリケーションと、TV録画のようなその他の処理を並行して行ったときの、CPUリソースの不足を防ぐことができる。

【0156】

上記各実施の形態の説明においては、暗号アルゴリズムのネゴシエーションについて説明したが、本発明は、認証アルゴリズムのネゴシエーションの場合にも適用できる。認証アルゴリズムは、受信したデータが伝送途中で改ざんされていないことを確認するアルゴリズムである。また、本発明は、暗号アルゴリズムに代わって、映像データ、音声データ、一般のデータなどの圧縮、伸長に関する圧縮アルゴリズムの折衝にも使用できる。データ圧縮のアルゴリズムとしては、DEFLATEやLZSなど種々のものがあるが、圧縮率、処理負荷と、そのときCPU使用率により、CPUリソースが枯渇しない範囲で、できるだけ圧縮率の高いアルゴリズムを選択することにより、通信回線への負荷を低減することができる。また、別の見方をすると、認証アルゴリズムの処理においては、もとの認証対象データに対して複雑な計算を行って認証データを生成し、また、圧縮アルゴリズムは、元のデータを圧縮データに変えて複雑な伸長処理を必要とする形にするという点では、暗号処理に類する点もあり、上記各実施の形態を、暗号アルゴリズムの選択に変えて、これらのアルゴリズムの選択に適用すること可能であ

る。

【図面の簡単な説明】

【図 1】

本発明の一実施の形態に関わるシステムの全体構成を示す図

【図 2】

ネットワークカメラと TV 録画を同時に動作させたときの CPU リソースの不足を示すグラフ

【図 3】

ネゴシエーションによる暗号アルゴリズム決定方法を示す図

【図 4】

実施の形態 1 において、レスポンドとして、暗号アルゴリズムのネゴシエーションを行うときの、暗号アルゴリズムネゴシエーション機能部の動作を示すフローチャート

【図 5】

図 4 の処理の一部分を詳細にしたフローチャート

【図 6】

暗号アルゴリズムによる CPU 使用率の違いを示すグラフ

【図 7】

暗号アルゴリズムと、その処理負荷、暗号強度との対応を保持するデータベースを示す図

【図 8】

実施の形態 1 において、イニシエータとして、暗号アルゴリズムのネゴシエーションを行うときの、暗号アルゴリズムネゴシエーション機能部の動作を示すフローチャート

【図 9】

図 8 の処理の一部分を詳細にしたフローチャート

【図 10】

実施の形態 2 において、レスポンドとして、暗号アルゴリズムのネゴシエーションを行うときの、暗号アルゴリズムネゴシエーション機能部の動作を示すフロ

ーチャート

【図 11】

図 10 の処理の一部分を詳細にしたフローチャート

【図 12】

実施の形態 2 において、イニシエータとして、暗号アルゴリズムのネゴシエーションを行うときの、暗号アルゴリズムネゴシエーション機能部の動作を示すフローチャート

【図 13】

図 12 の処理の一部分を詳細にしたフローチャート

【図 14】

実施の形態 3 において、CPU 使用率が変化したタイミングで、イニシエータとして暗号アルゴリズムのネゴシエーションを行うときの、暗号アルゴリズムネゴシエーション機能部の動作を示すフローチャート

【図 15】

図 14 の処理の一部分を詳細にしたフローチャート

【図 16】

実施の形態 4 において、複数の暗号アルゴリズムがあらかじめネゴシエーションされている場合の、処理フローを示すフローチャート

【図 17】

図 16 の処理の一部分を詳細にしたフローチャート

【図 18】

ep サービスのしくみを示す図

【図 19】

本発明のネゴシエーションを行なう一実施の形態の要部のブロック図

【図 20】

ネゴシエーションを行なう従来例の要部のブロック図

【符号の説明】

100 放送設備

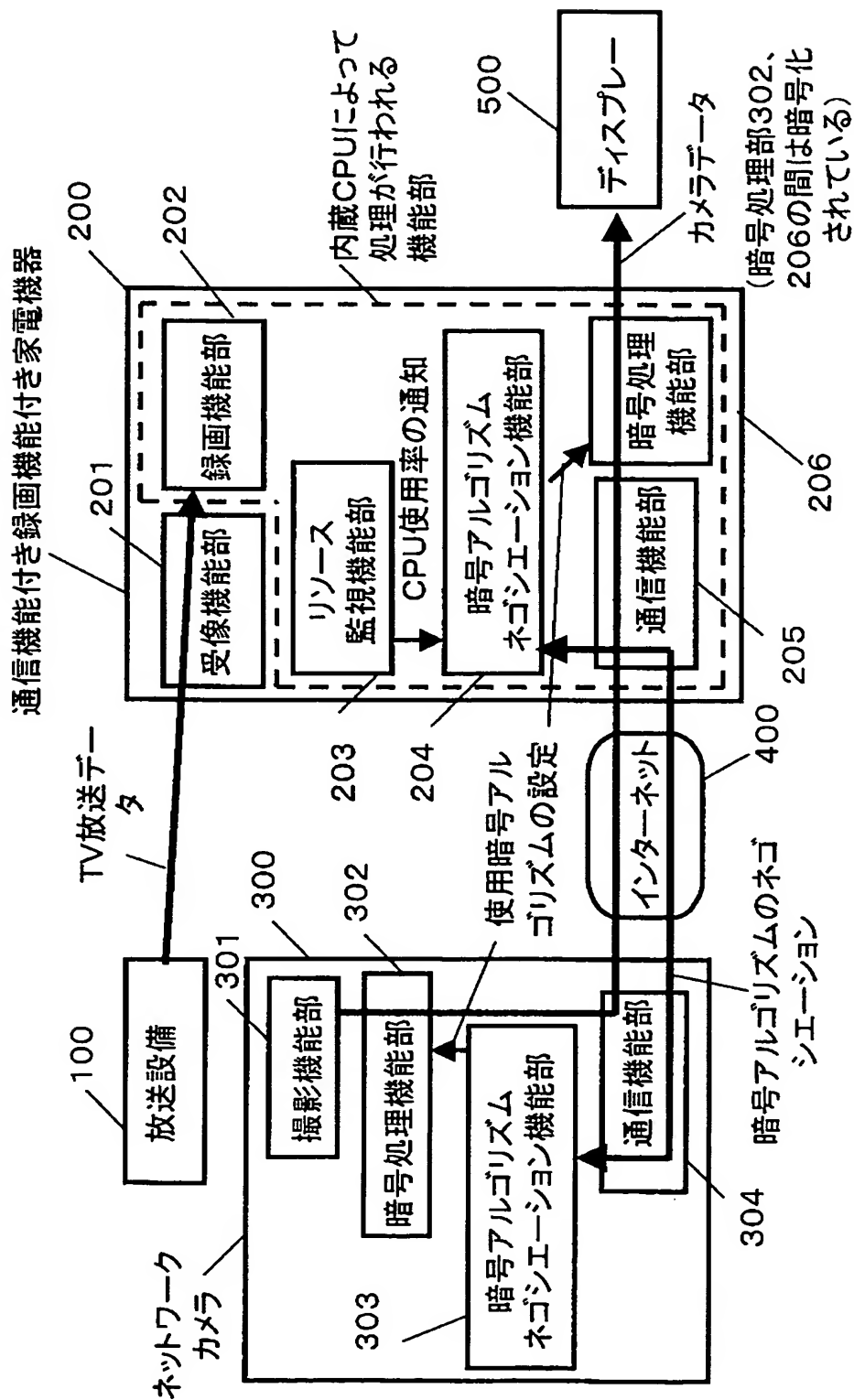
200 通信機能付き録画機能付き家電機器

- 3 0 0 ネットワークカメラ
- 4 0 0 インターネット
- 5 0 0 ディスプレー
- 2 0 1 受像機能部
- 2 0 2 録画機能部
- 2 0 3 リソース監視機能部
- 2 0 4 (通信機能付き録画機能付き家電機器内の) 暗号アルゴリズムネゴシエーション機能部
- 2 0 5 (通信機能付き録画機能付き家電機器内の) 通信機能部
- 2 0 6 (通信機能付き録画機能付き家電機器内の) 暗号処理機能部
- 3 0 1 撮影機能部
- 3 0 2 (ネットワークカメラ内の) 暗号処理機能部
- 3 0 3 (ネットワークカメラ内の) 暗号アルゴリズムネゴシエーション機能部
- 3 0 4 (ネットワークカメラ内の) 通信機能部

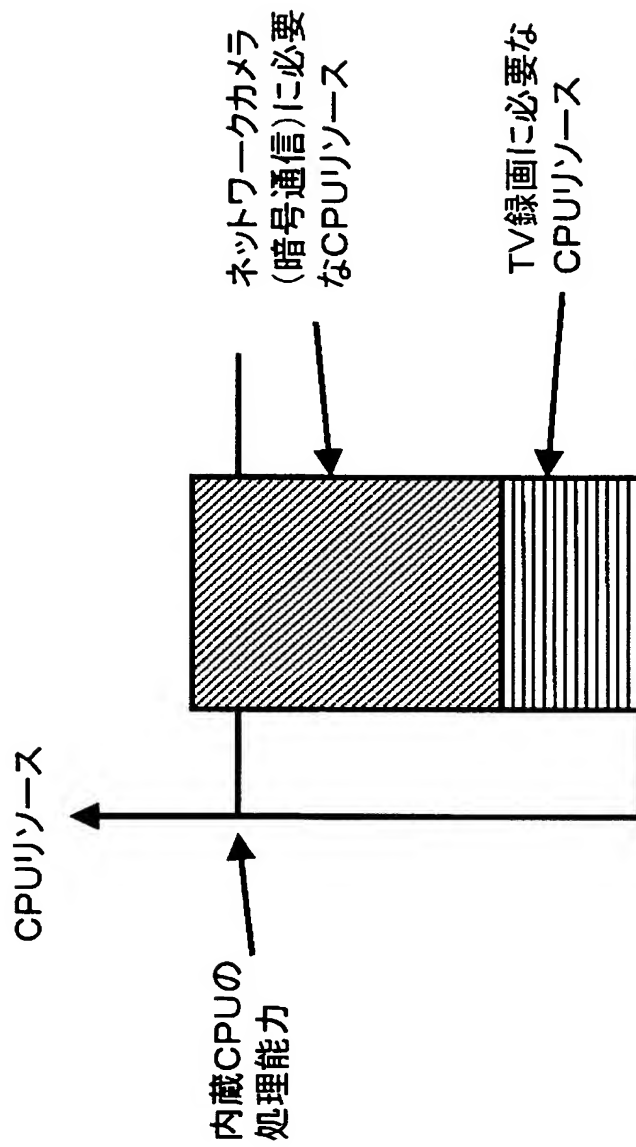
【書類名】

図面

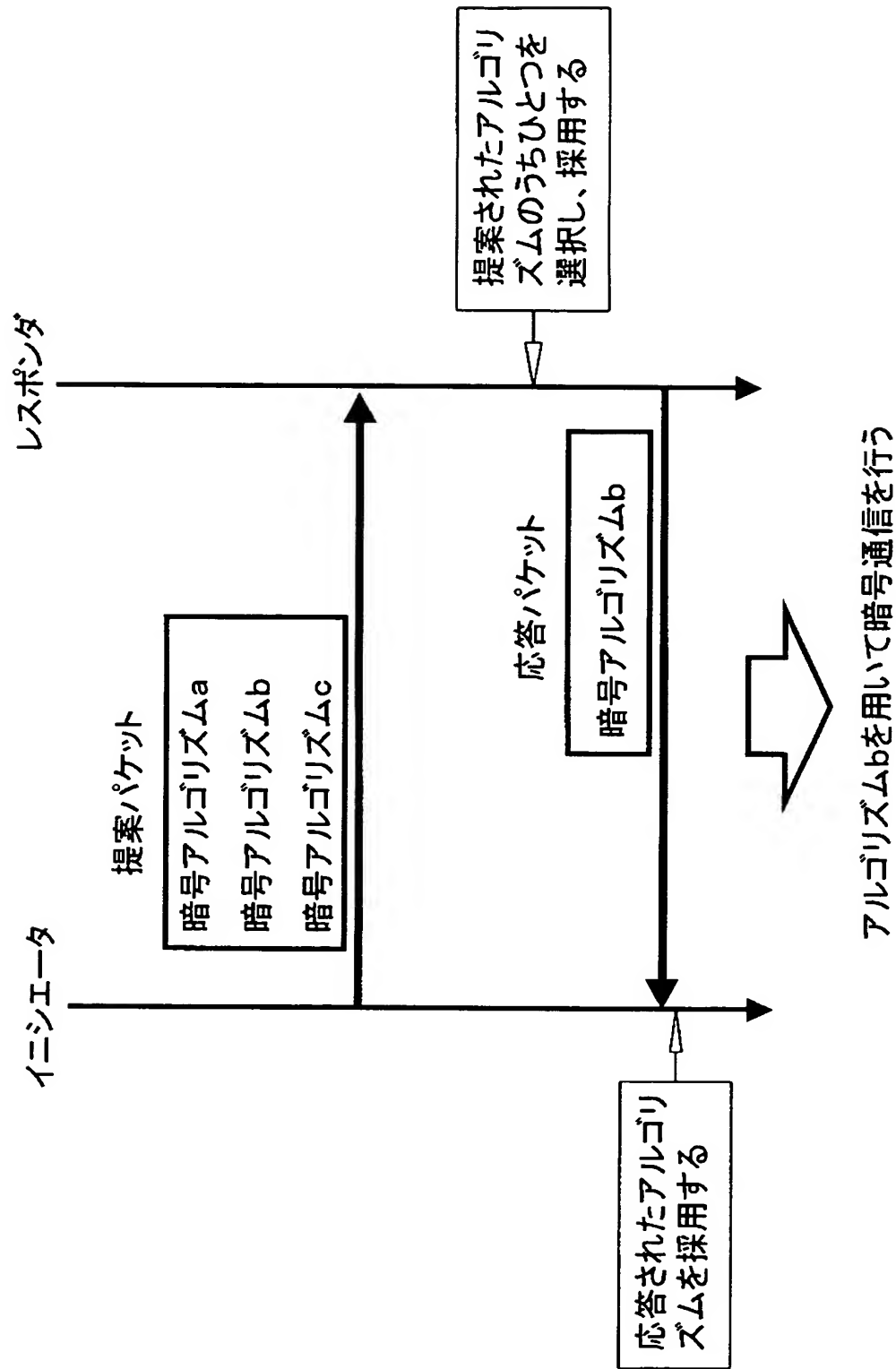
【図 1】



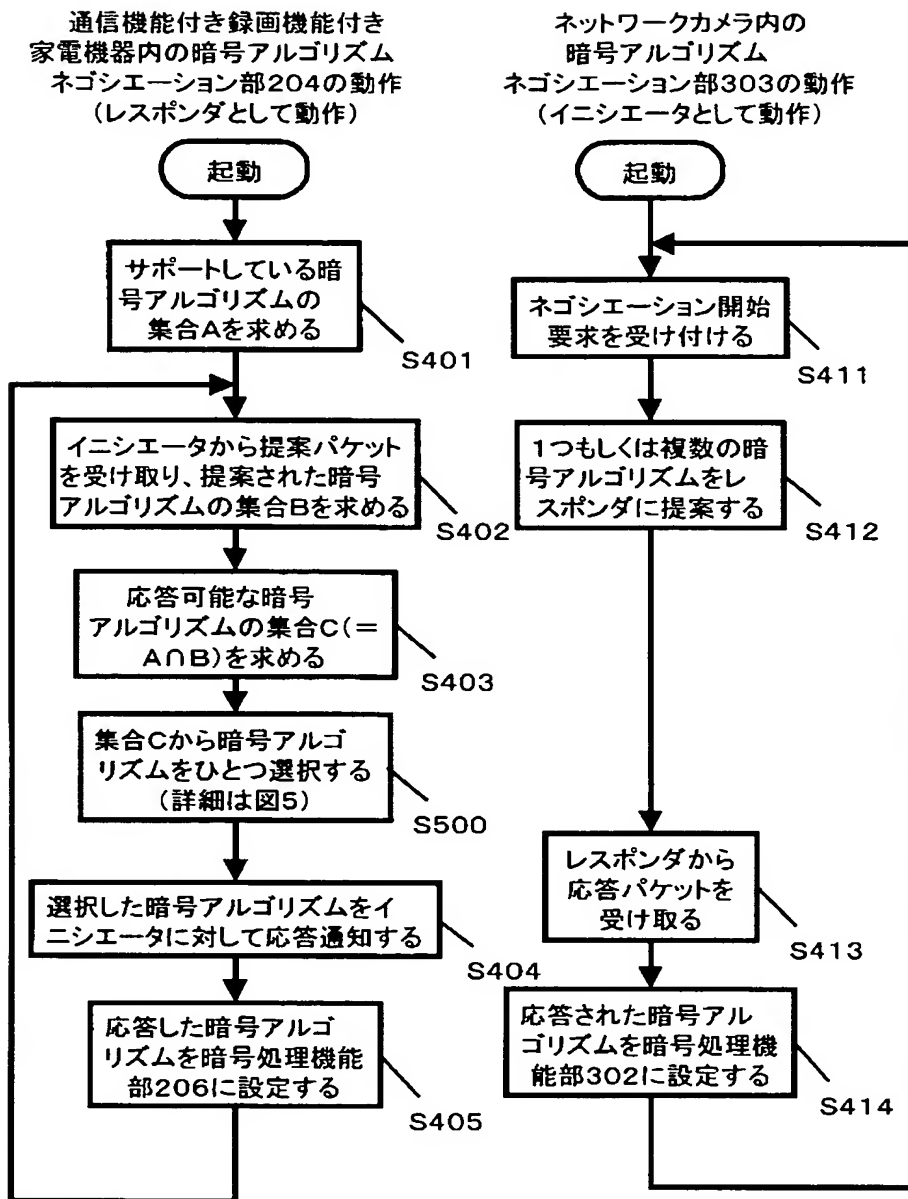
【図 2】



【図 3】

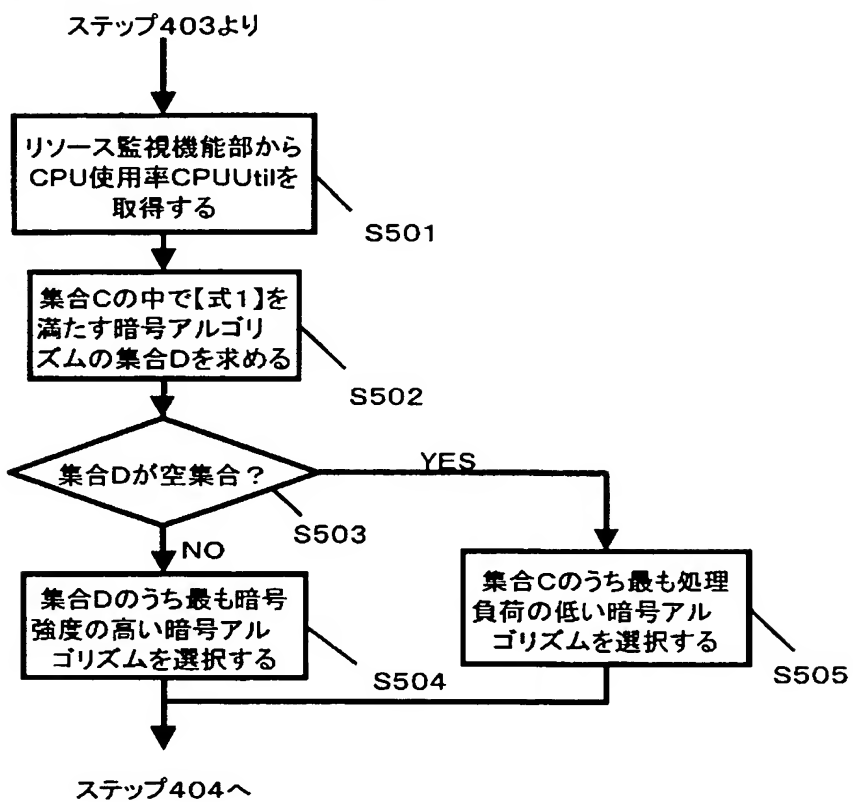


【図 4】



【図 5】

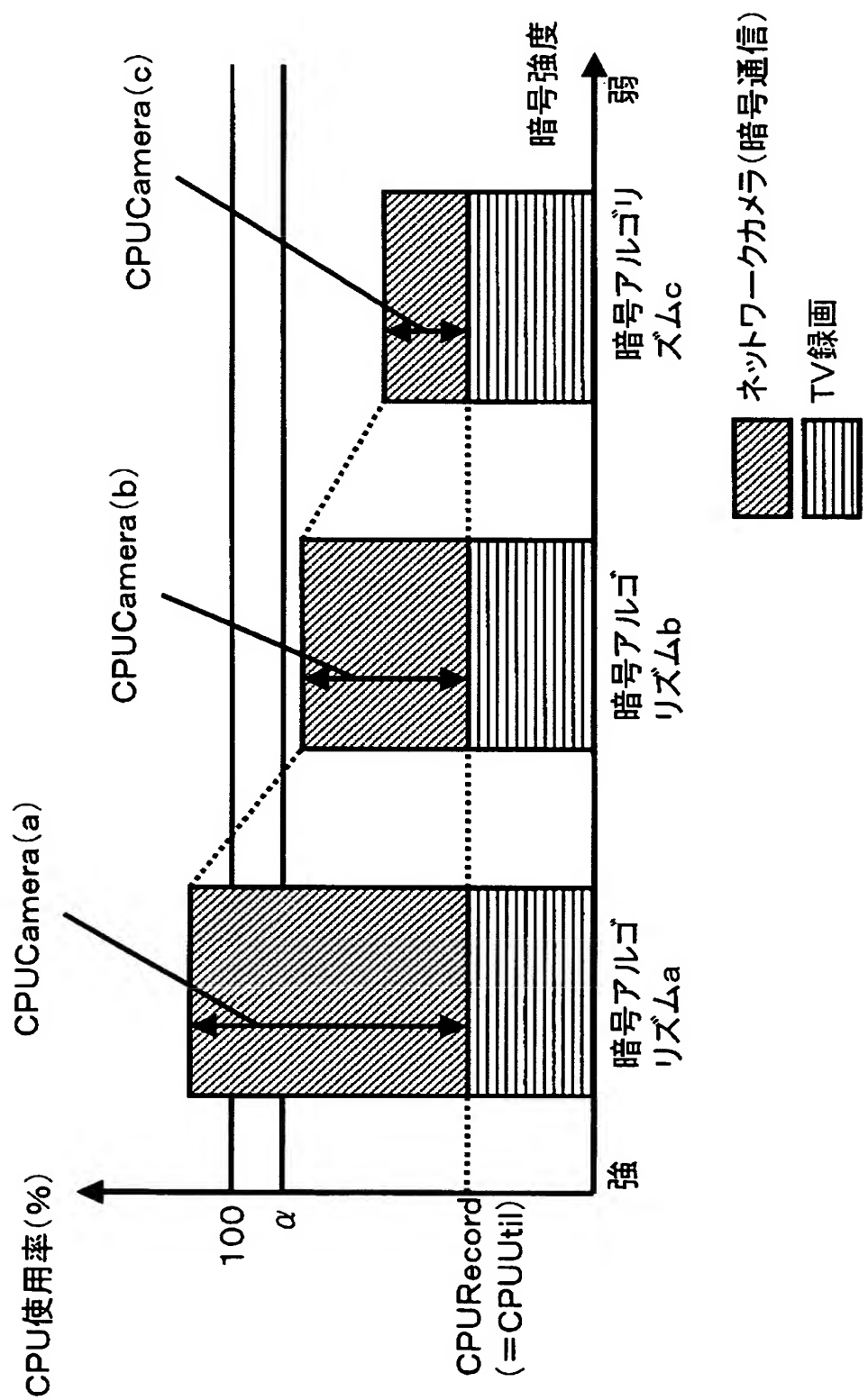
図4ステップ500の詳細



$$\text{【式1】: CPURecord} + \text{CPUCamera}(x) \leq \alpha$$

CPUCamera(x): 暗号アルゴリズムxを用いたときに
ネットワークカメラアプリケーションが
消費するCPUリソース

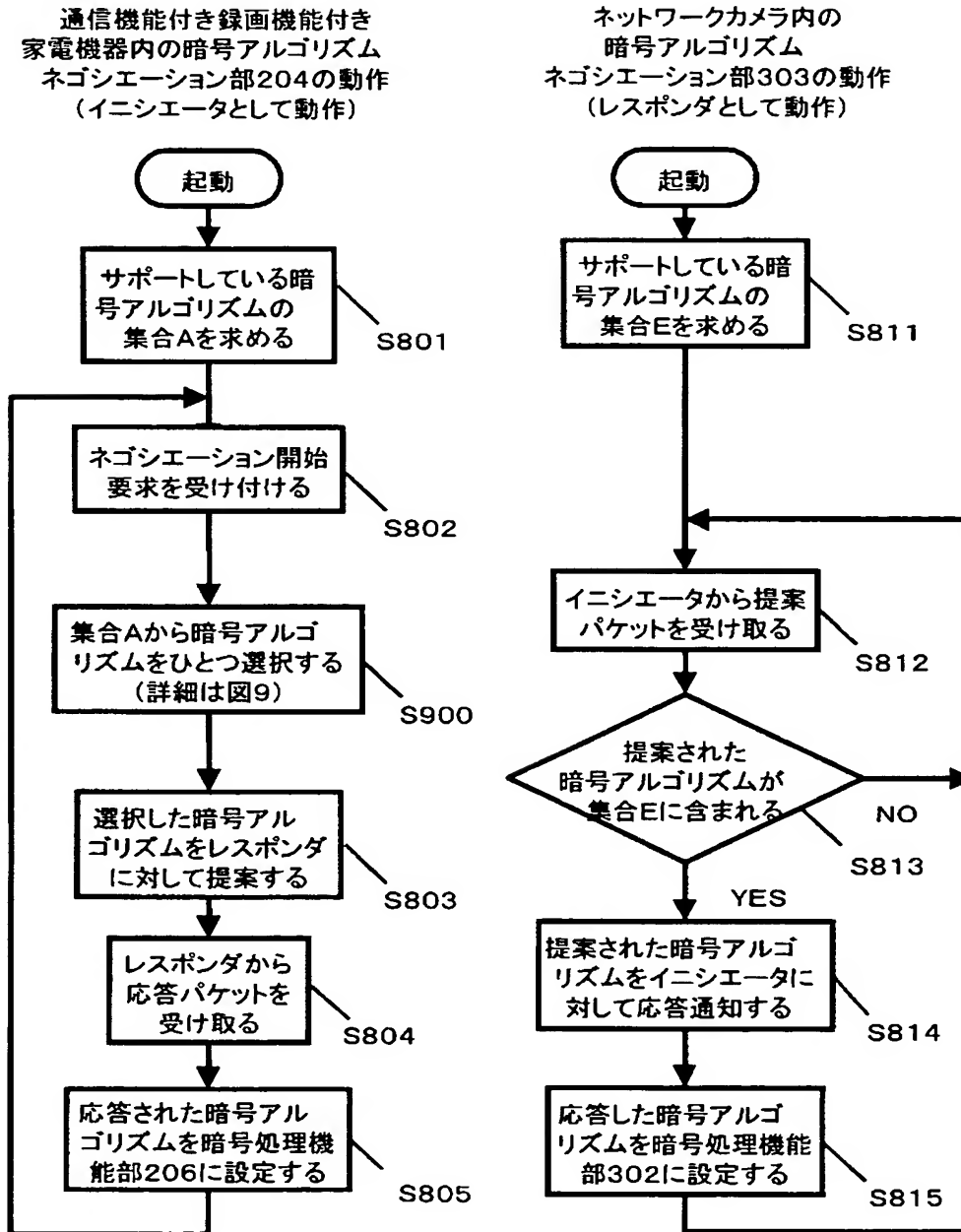
【図 6】



【図 7】

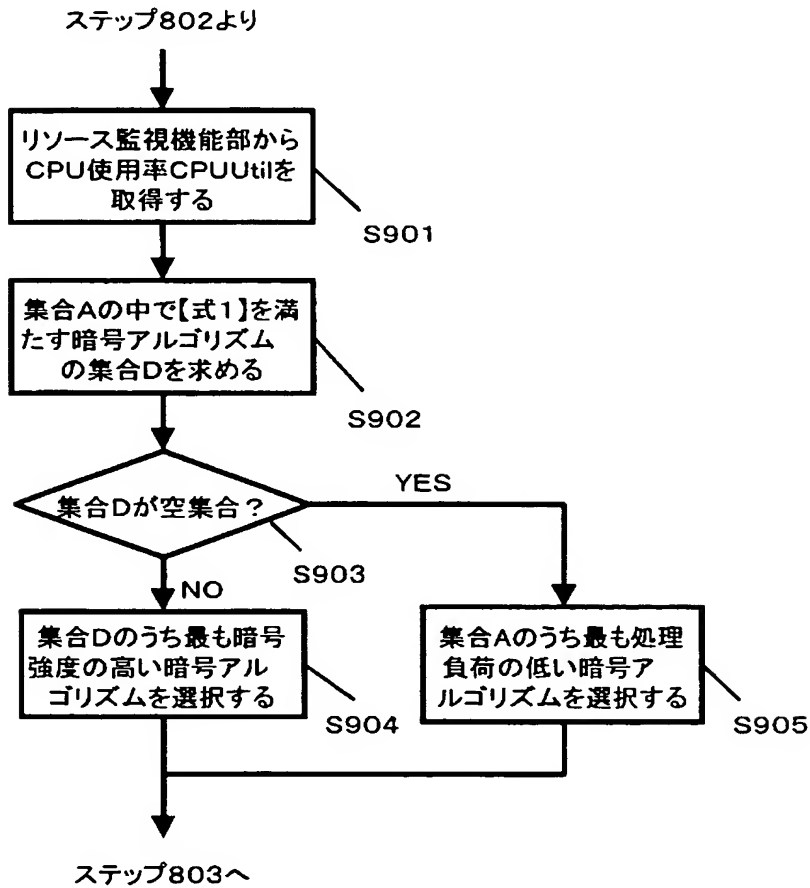
暗号アルゴリズム	EncRate()	暗号強度
a	20	1
b	40	2
c	70	3
:	:	:

【図 8】



【図 9】

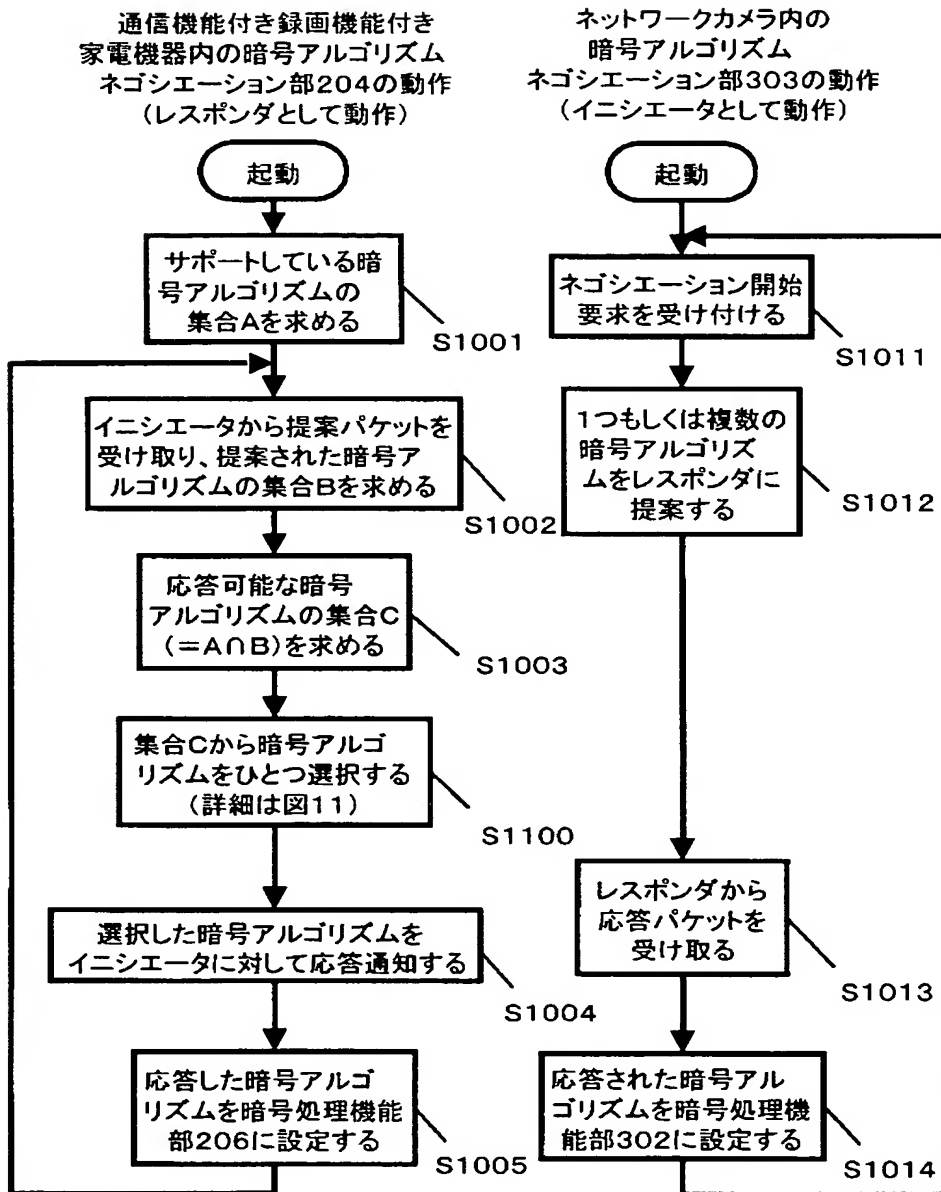
図8ステップ900の詳細



【式1】: $\text{CPURecord} + \text{CPUTCamera}(x) \leq \alpha$

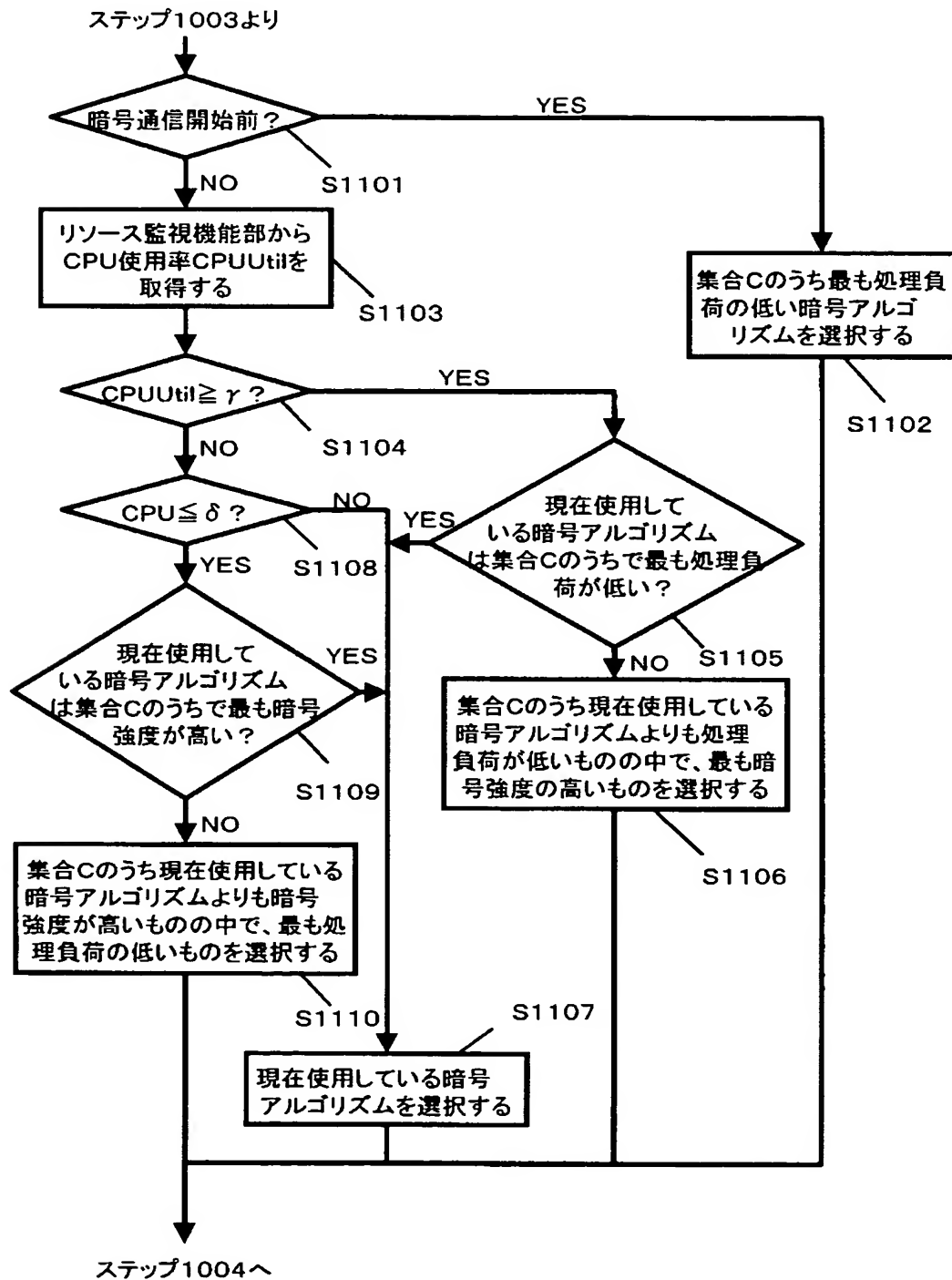
$\text{CPUTCamera}(x)$: 暗号アルゴリズム x を用いたときに
ネットワークカメラアプリケーションが
消費するCPUリソース

【図 10】

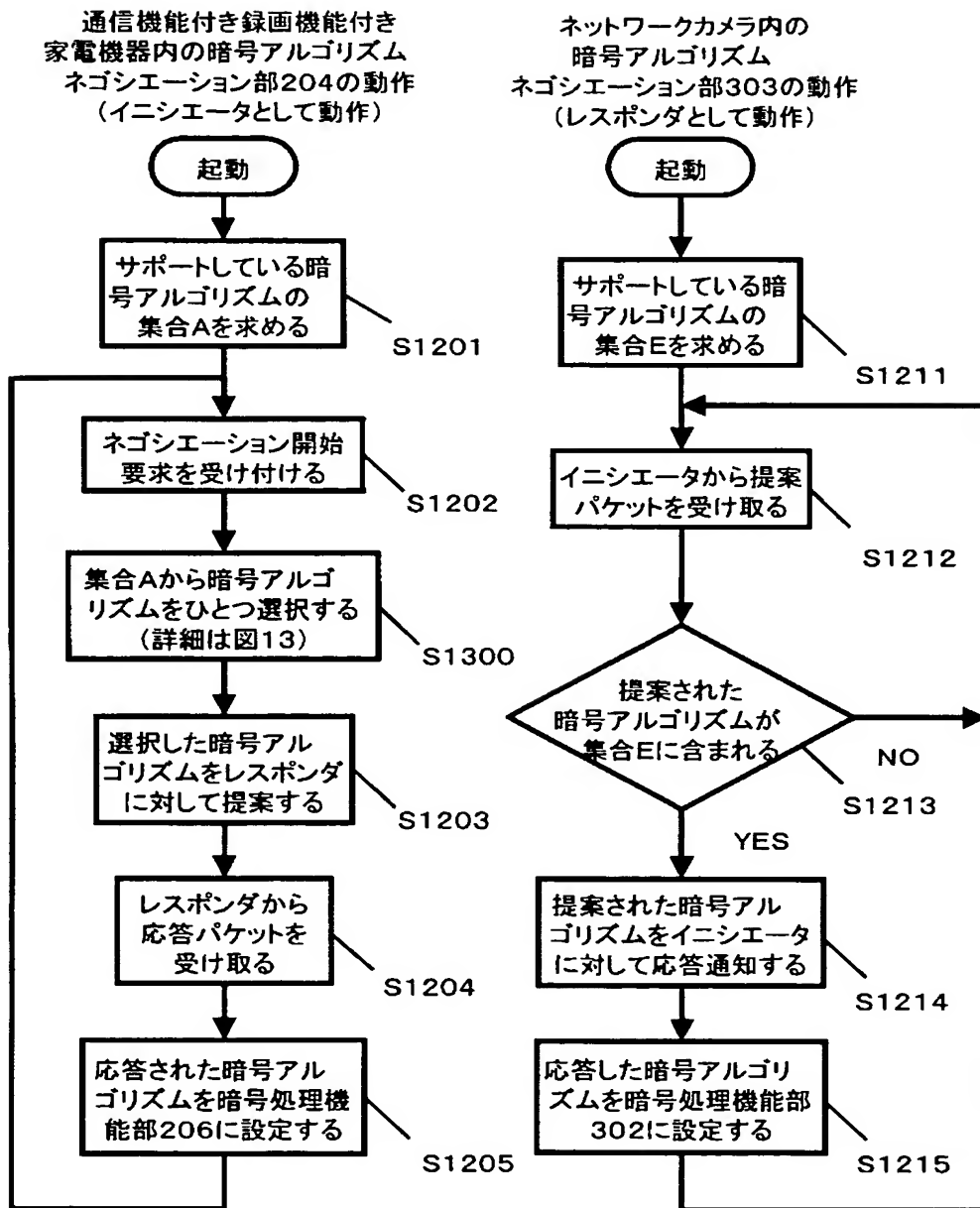


【図11】

図10ステップ1100の詳細

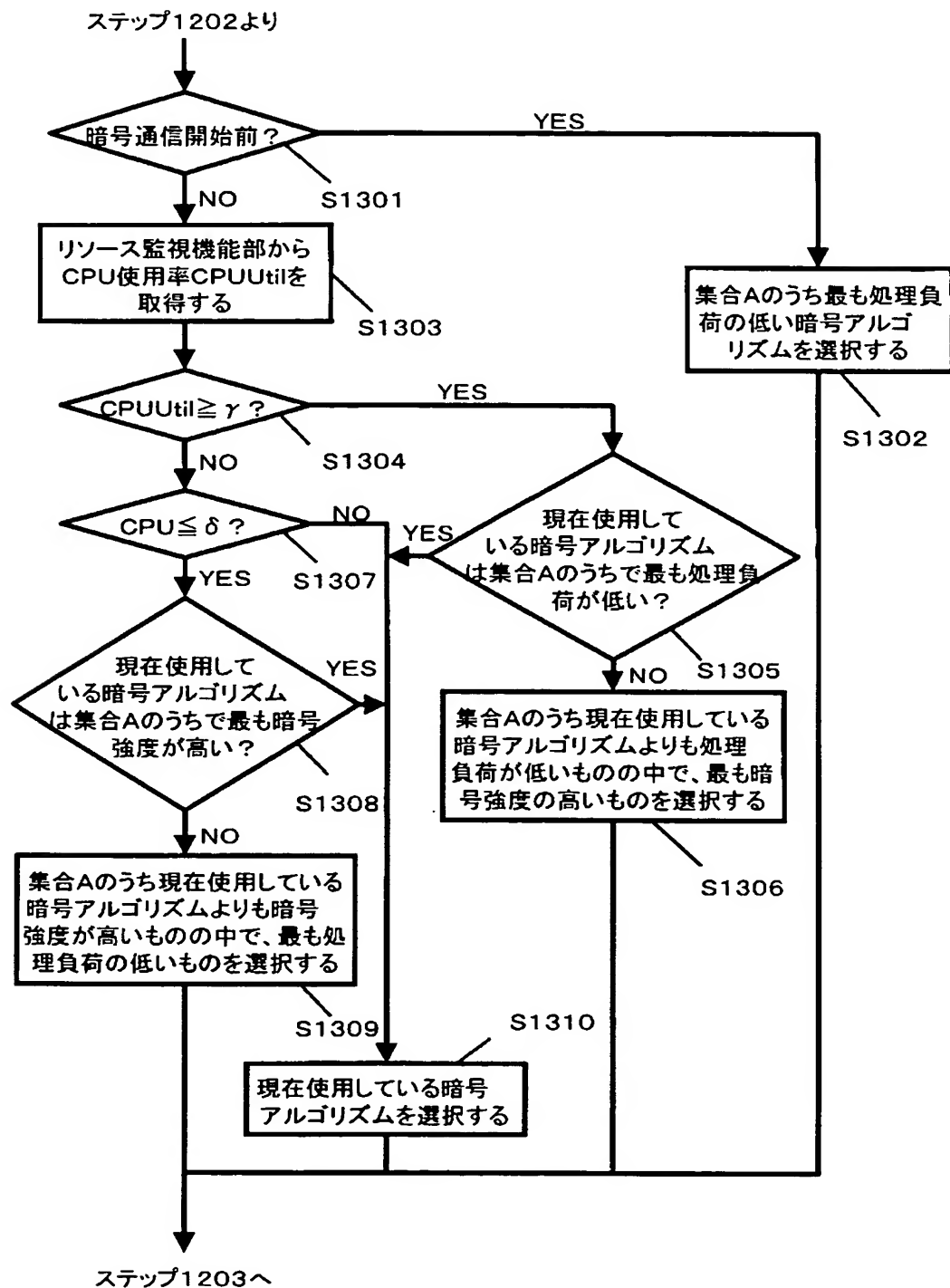


【図 12】

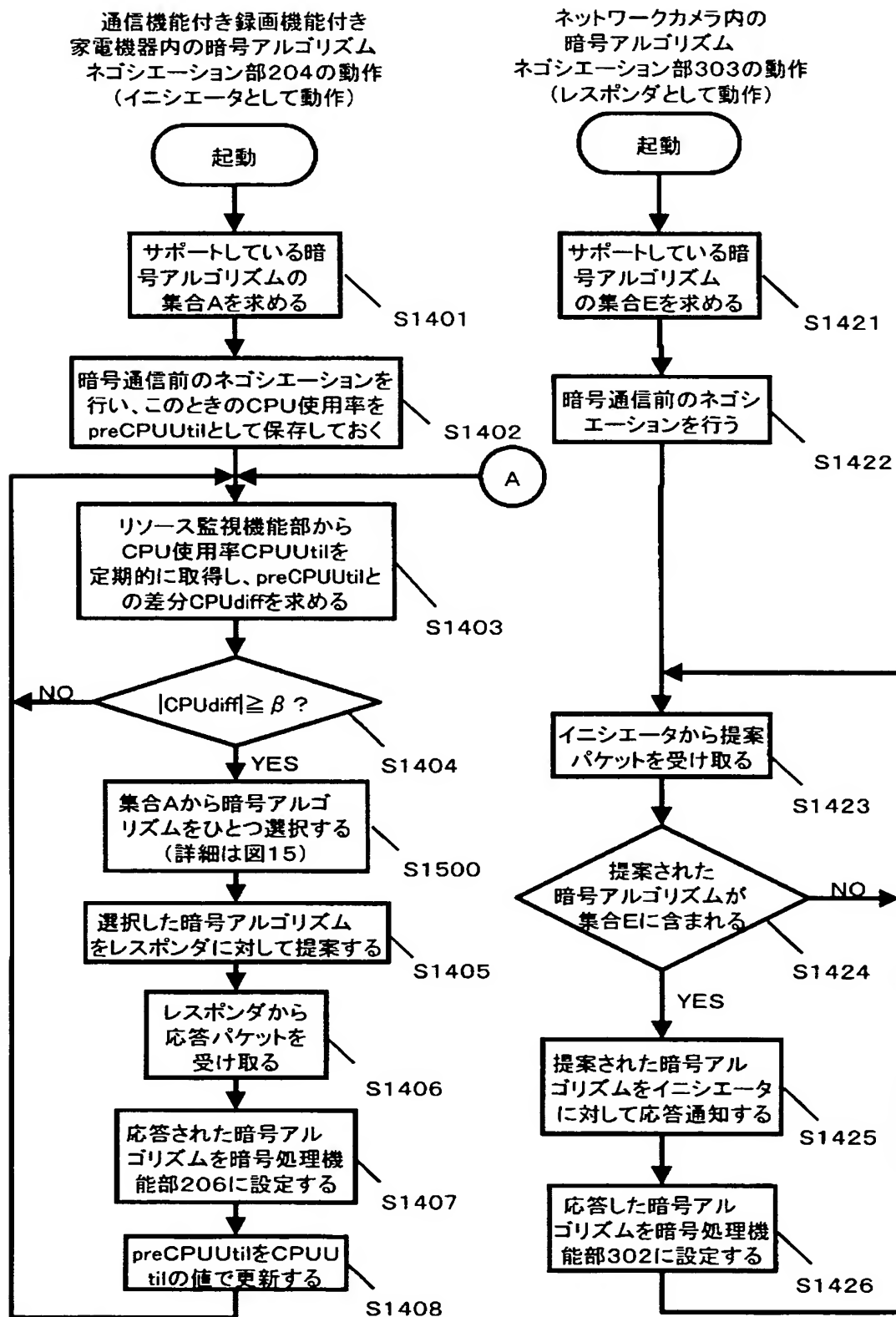


【図 13】

図12ステップ1300の詳細

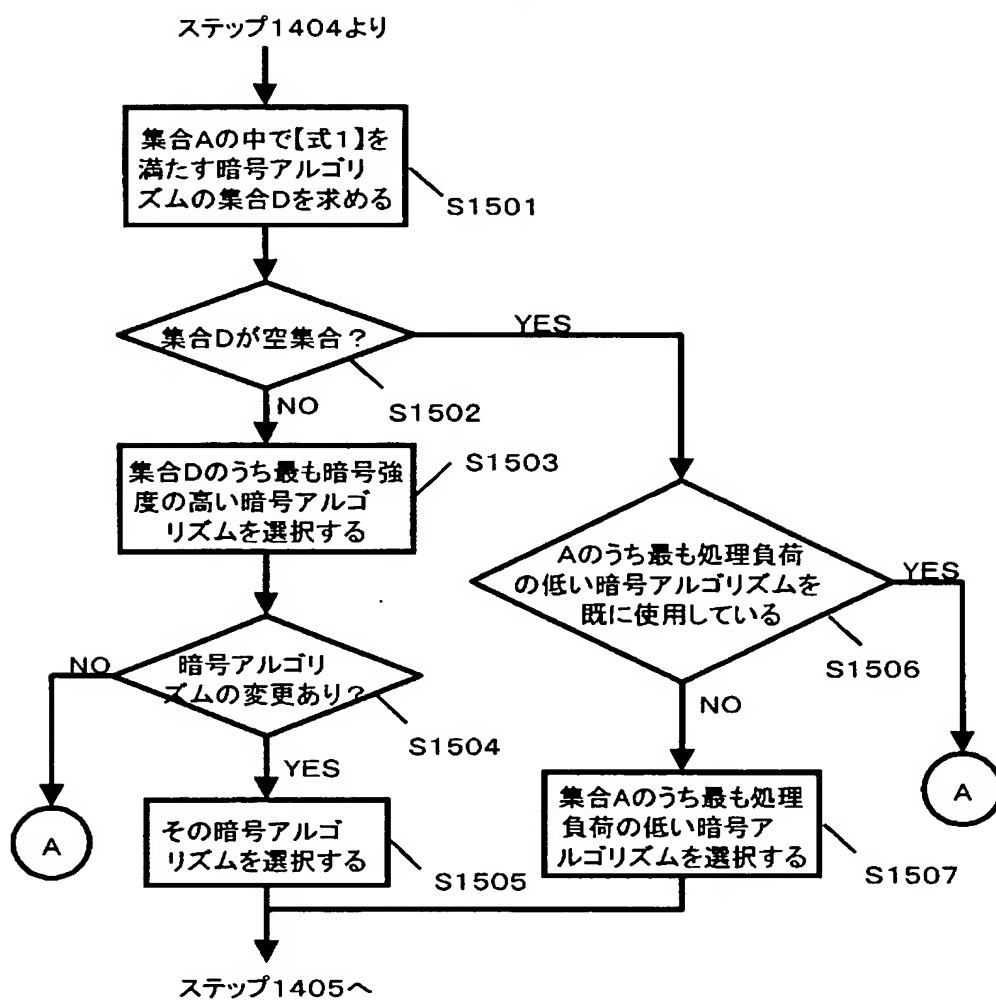


【図 14】



【図15】

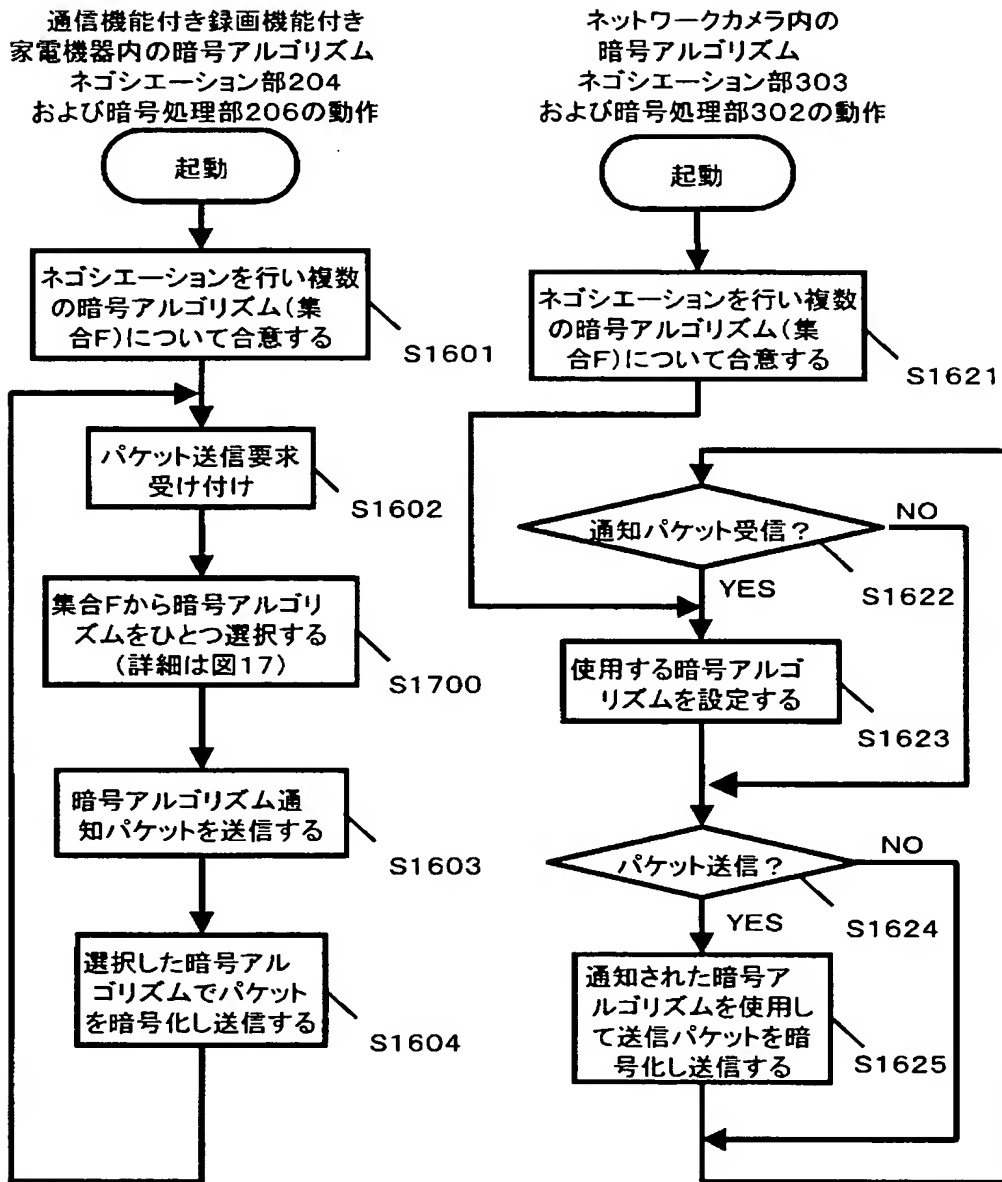
図14ステップ1500の詳細



【式1】: $CPURecord + CPUCamera(x) \leq \alpha$

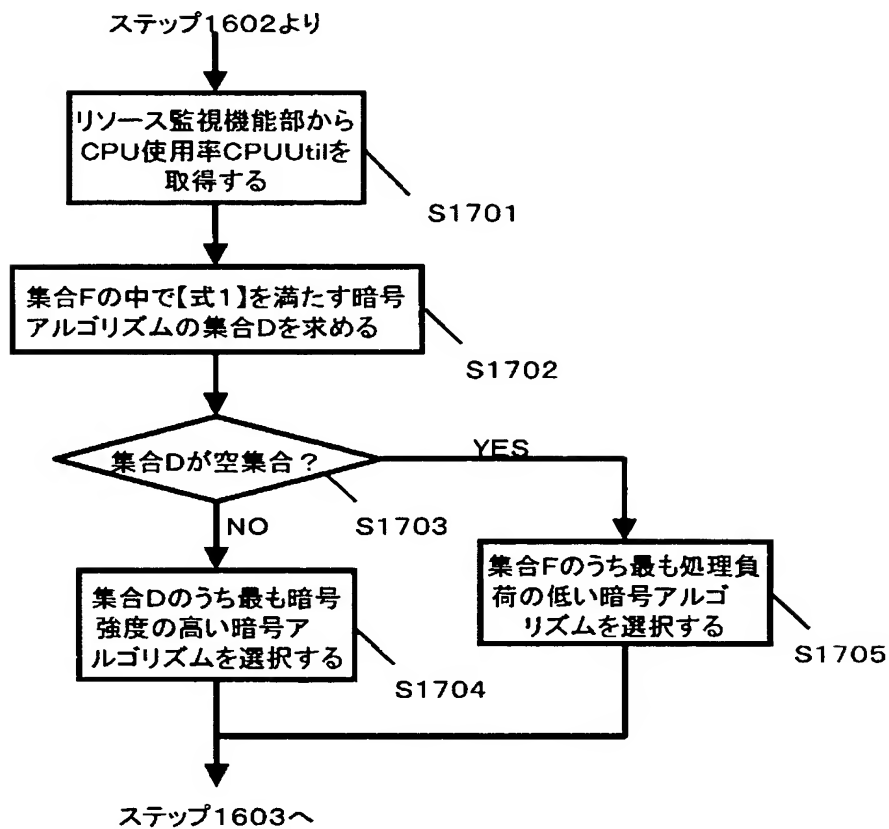
$CPUCamera(x)$: 暗号アルゴリズム x を用いたときに
ネットワークカメラアプリケーションが
消費するCPUリソース

【図16】



【図 17】

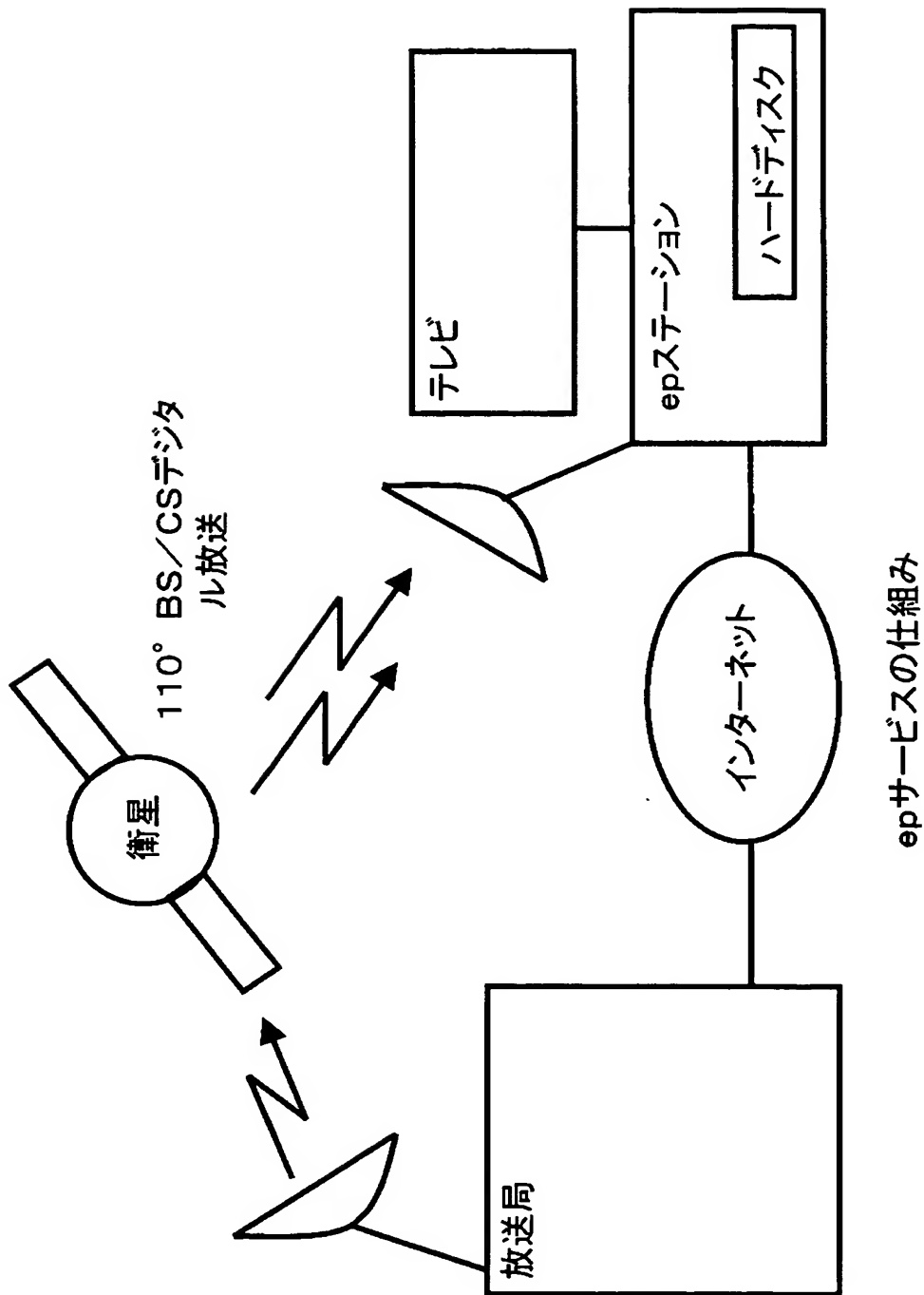
図16ステップ1700の詳細



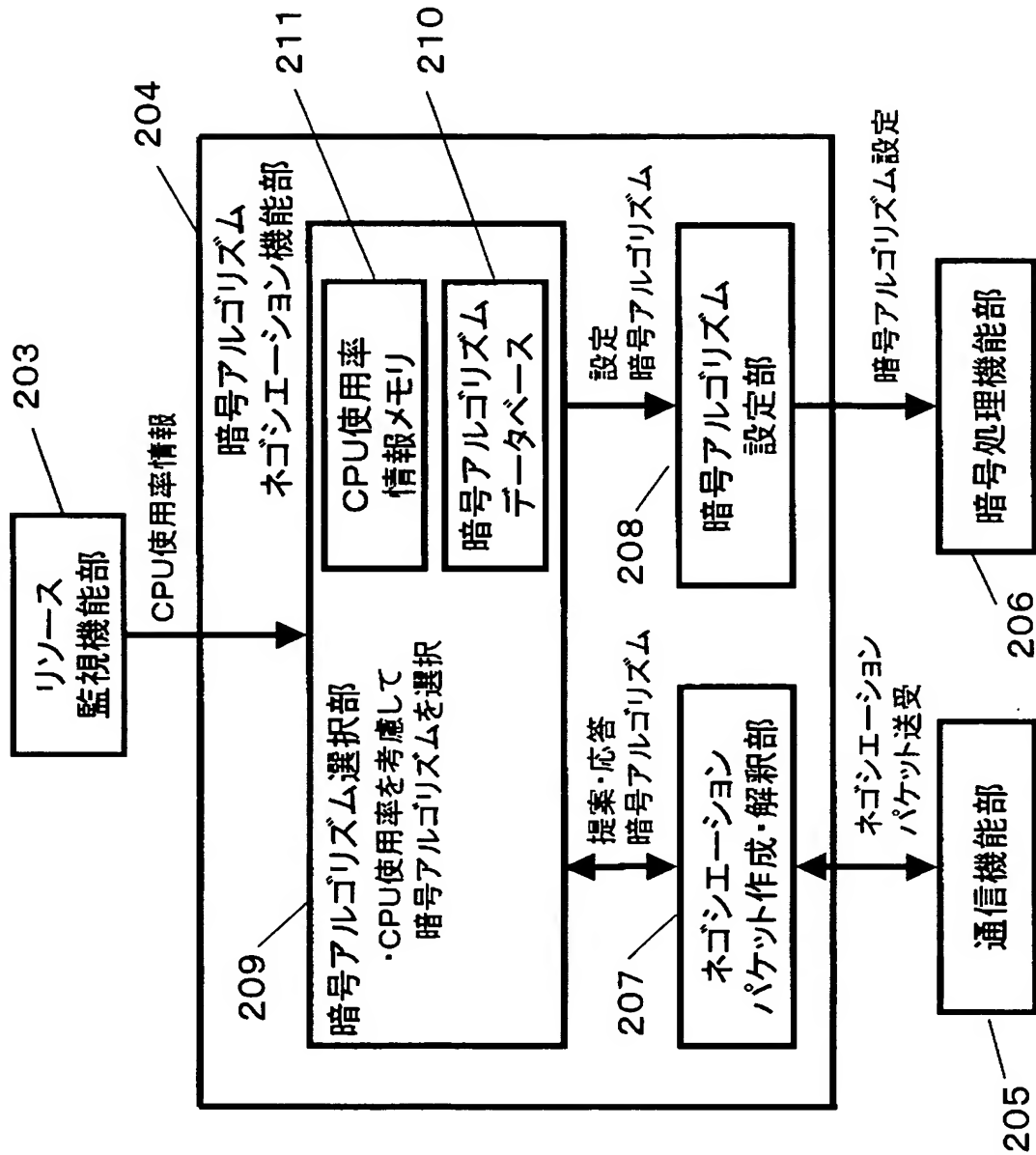
【式1】: $\text{CPURecord} + \text{CPUTCamera}(x) \leq \alpha$

$\text{CPUTCamera}(x)$: 暗号アルゴリズム x を用いたときに
ネットワークカメラアプリケーションが
消費するCPUリソース

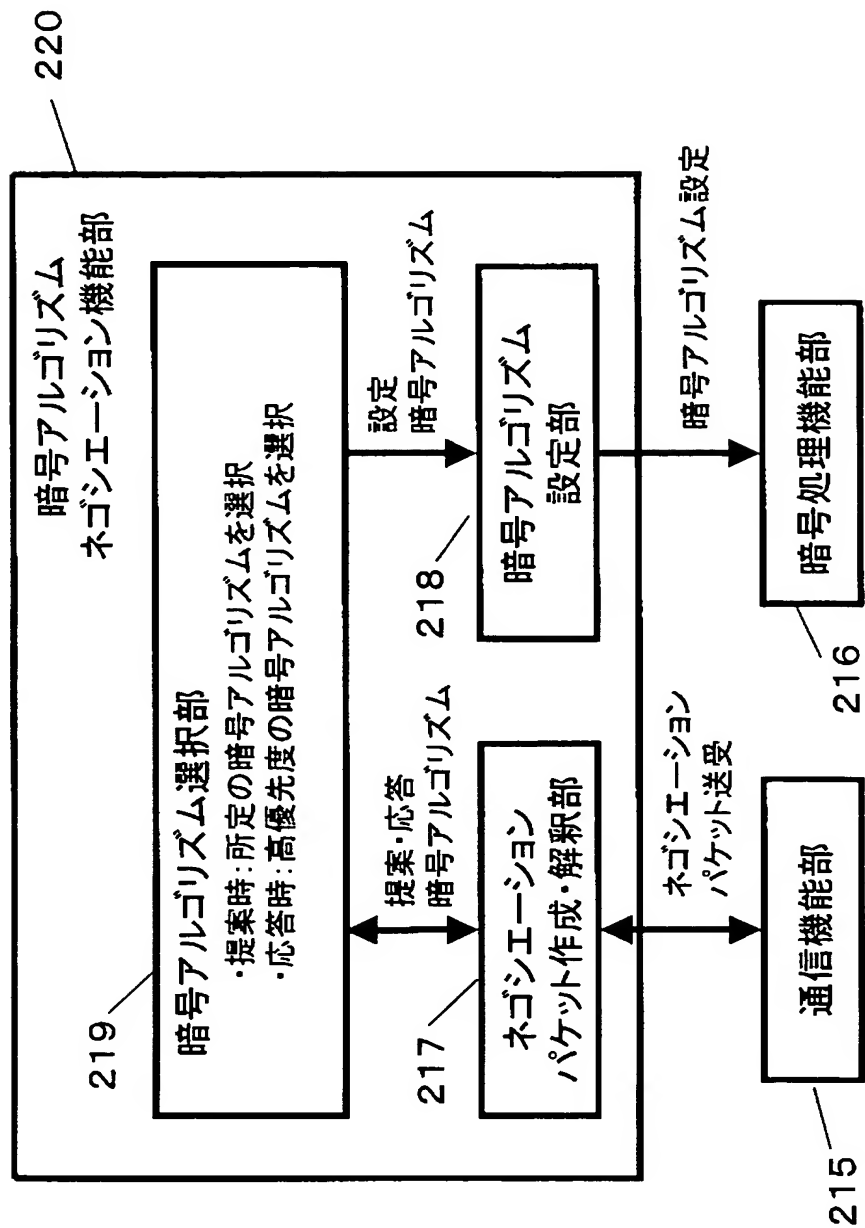
【図 18】



【図 19】



【図 20】



従来

【書類名】 要約書

【要約】

【課題】 暗号、認証などの処理と他の高負荷な処理を同時に行った場合、CPUリソースが不足するという問題が起こり得る。例えば、ネットワークカメラなどの暗号通信処理と、TV録画などの高負荷な処理を同時に行った場合、どちらかの処理が正常に行えない場合がある。このような場合においても、両方の処理をリアルタイムに正常に行えるような、暗号、認証などのアルゴリズムを選択する方法を提供することである。

【解決手段】 通信及び録画機能付き家電機器内の暗号アルゴリズムネゴシエーション機能部204は通信相手のネットワークカメラ内の同機能部303と暗号通信に利用する暗号、認証等のアルゴリズムを折衝する。この時、CPU負荷に応じて、選択する暗号、認証などのアルゴリズムを変化させる。すなわち、CPU使用率が高い場合には、低負荷の暗号、認証等のアルゴリズムを選択し、その暗号、認証などのアルゴリズムを用いて暗号通信を行う。

【選択図】 図1

特願 2 0 0 2 - 3 1 8 1 8 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1 . 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社